

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年3月29日 (29.03.2001)

PCT

(10) 国際公開番号
WO 01/22242 A1

(51) 国際特許分類: G06F 15/00, G10K 15/02

[JP/JP]: 〒141-0001 東京都品川区北品川6丁目7番35
号 ソニー株式会社内 Tokyo (JP).

(21) 国際出願番号: PCT/JP00/06308

(22) 国際出願日: 2000年9月14日 (14.09.2000)

(74) 代理人: 佐藤隆久 (SATO, Takahisa); 〒111-0052 東京都台東区柳橋2丁目4番2号 宮木ビル4階 創造国際
特許事務所 Tokyo (JP).

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(81) 指定国 (国内): CN, KR, US.

(30) 優先権データ:
特願平11/309721 1999年9月17日 (17.09.1999) JP
特願平11/309722 1999年9月17日 (17.09.1999) JP

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

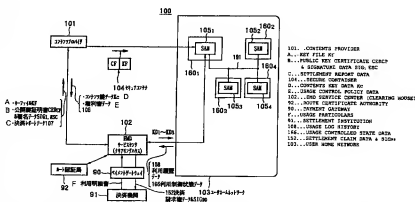
添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

(72) 発明者: および
(75) 発明者/出願人 (米国についてのみ): 野中 聡 (NON-
AKA, Akira) [JP/JP]. 江崎 正 (EZAKI, Tadashi)

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: DATA PROVIDING SYSTEM AND METHOD THEREFOR

(54) 発明の名称: データ提供システムおよびその方法



(57) Abstract: A data providing system capable of protecting the benefits of the people concerned about a data providing device. A contents provider (101) distributes a secure container (104) containing contents data encrypted with a contents key, contents key data encrypted with distribution key data, and encrypted usage control policy data representing the handling of the contents data to, e.g. an SAM (105), in a user home network (103). The SAM (105),

decodes the contents key data and the usage control policy data contained in the secure container (104) and determines the handling such as purchase form and usage form of the contents data according to the decoded usage control policy data.

[続業者]

WO 01/22242 A1

FIG.105

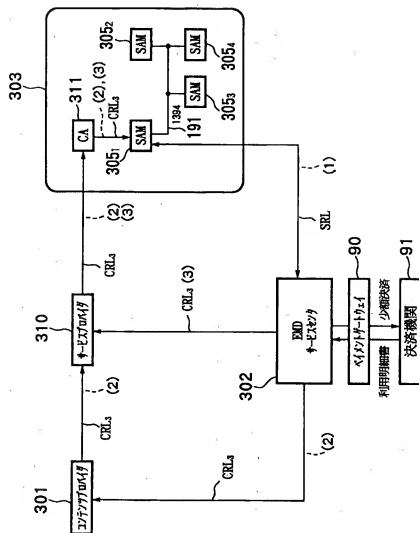


FIG.106

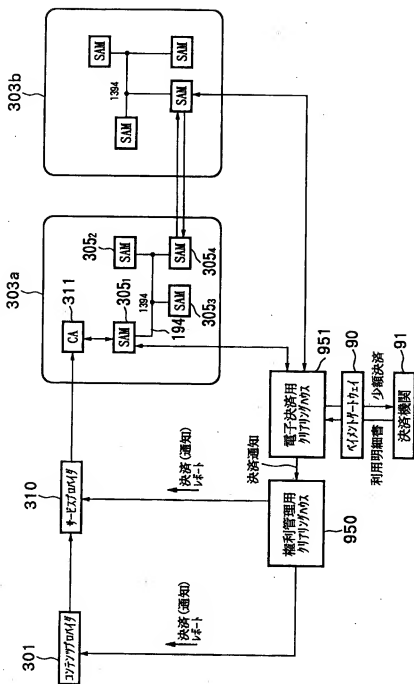


FIG.107

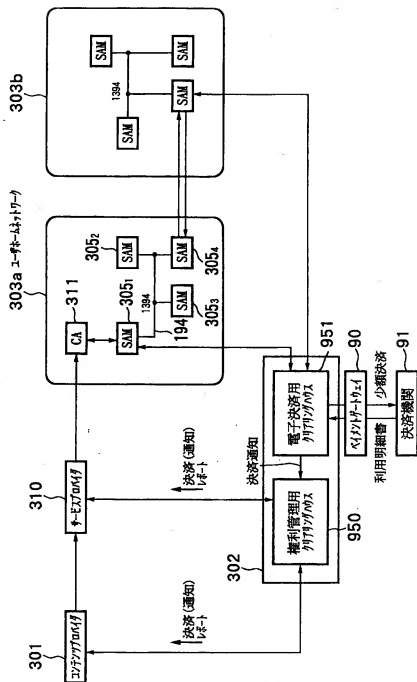


FIG.108

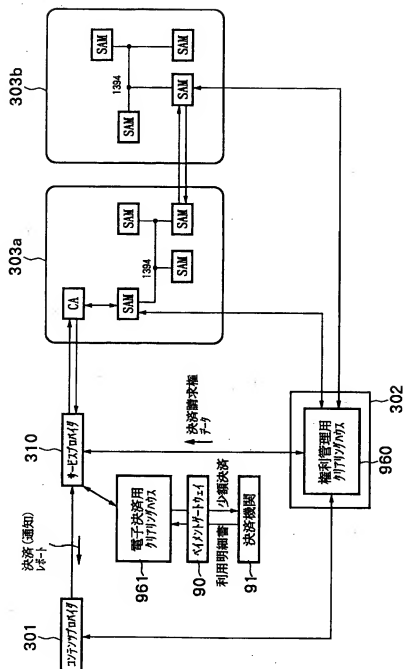


FIG.109

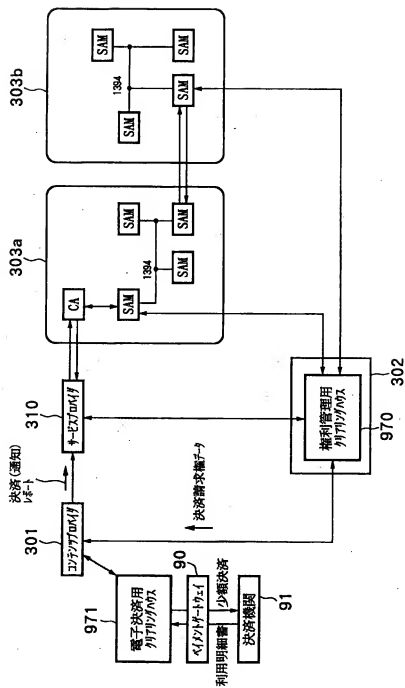


FIG.111

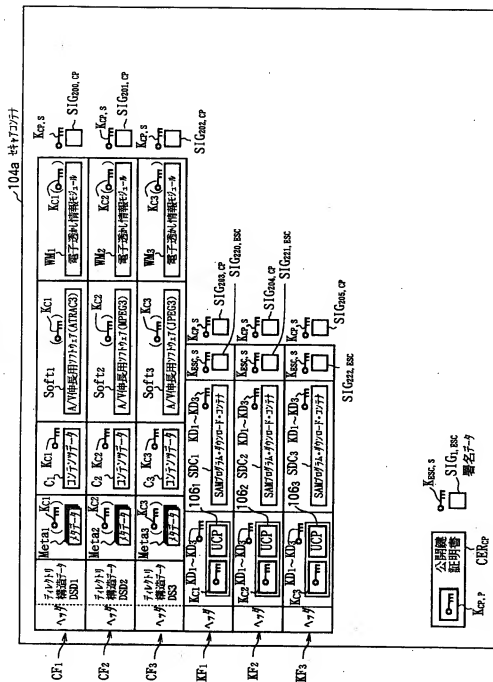


FIG.112

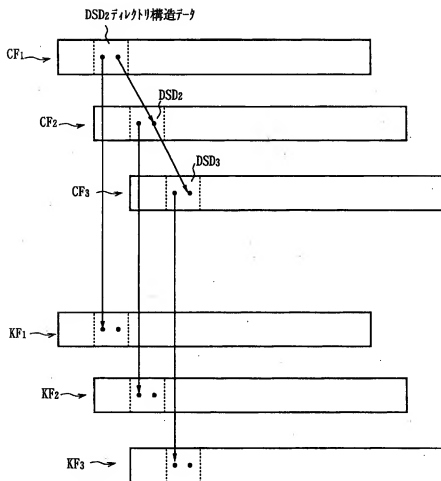


FIG.113

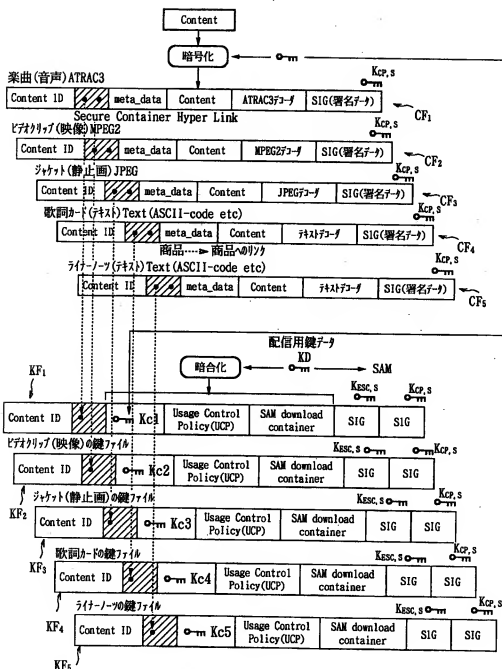


FIG.114

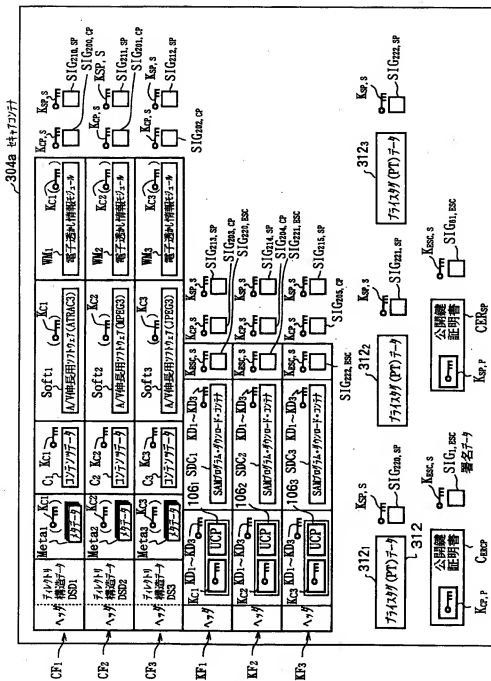


FIG.115

基本構成(識別情報型)のデータ①

基本構成

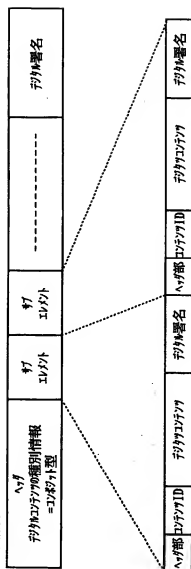


FIG.117

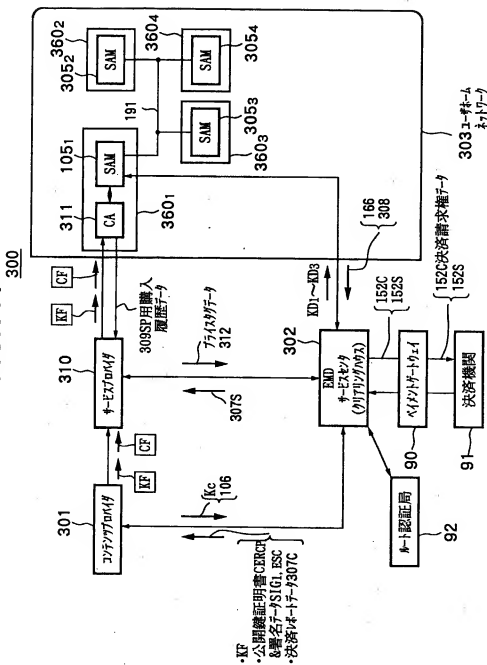


FIG.119

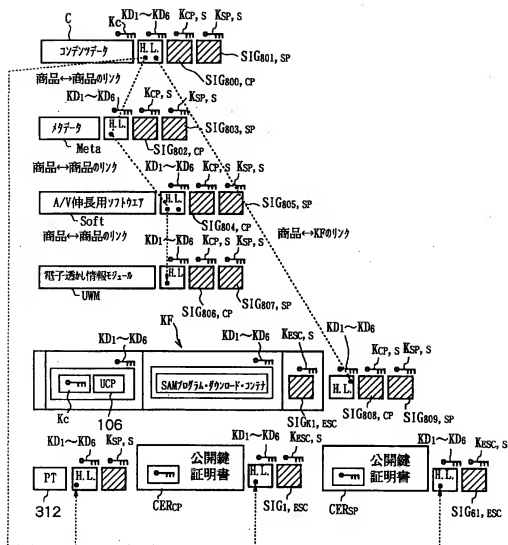


FIG.122

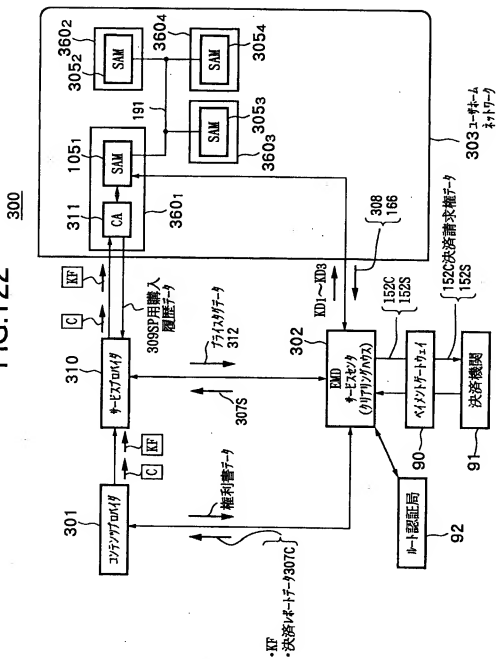


FIG. 124

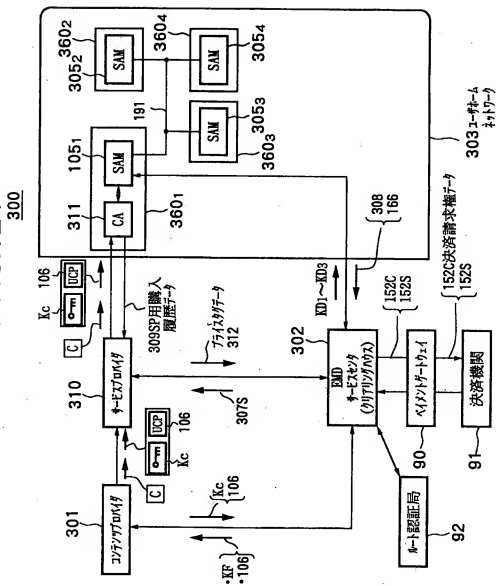


FIG. 125

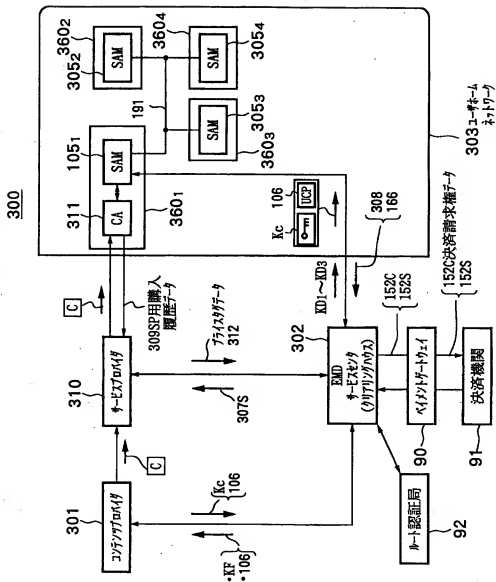


FIG.129

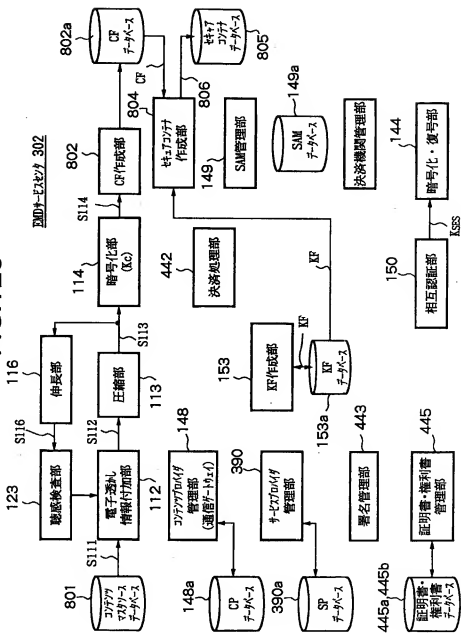


FIG.130

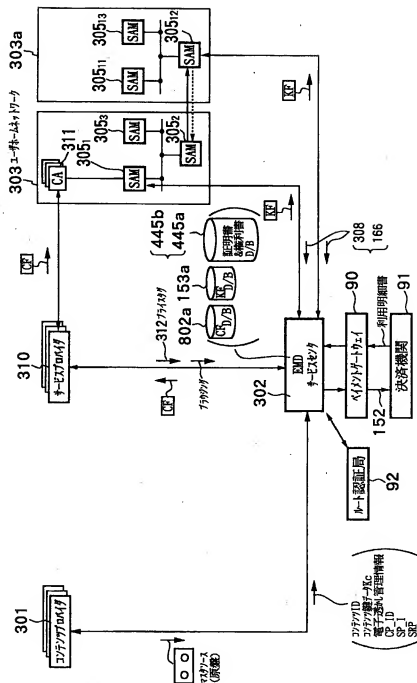


FIG.131

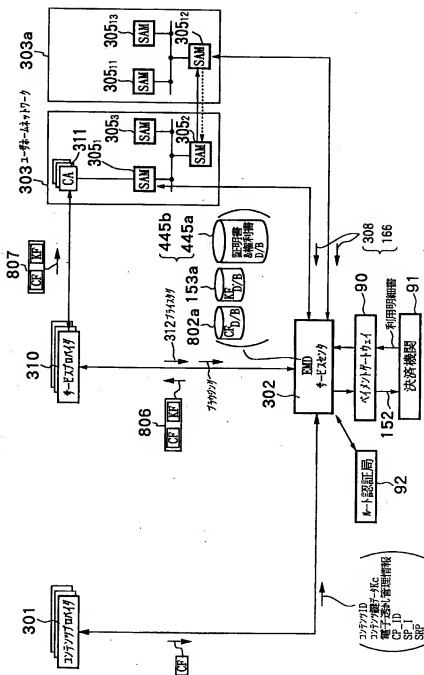


FIG.132

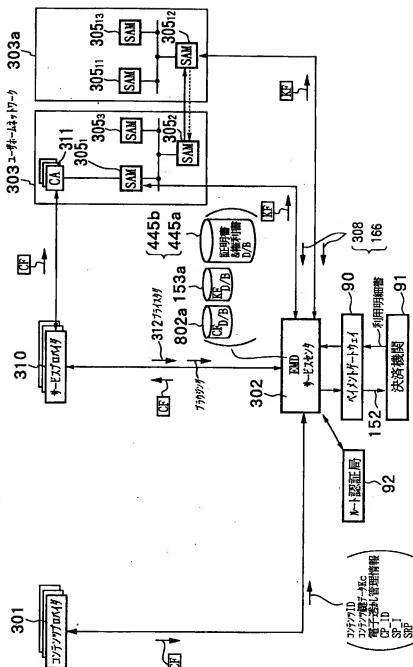


FIG.134

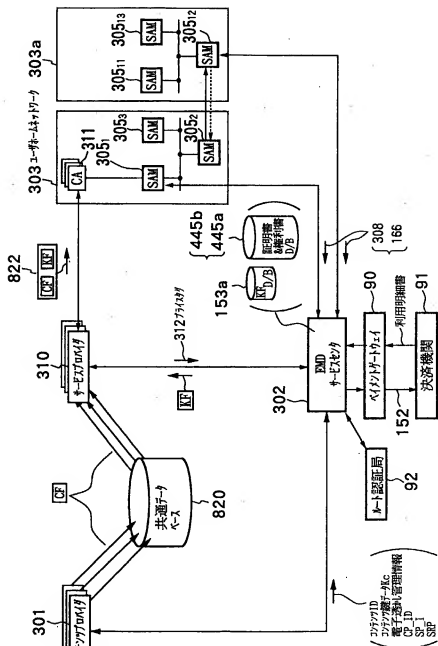


FIG.142

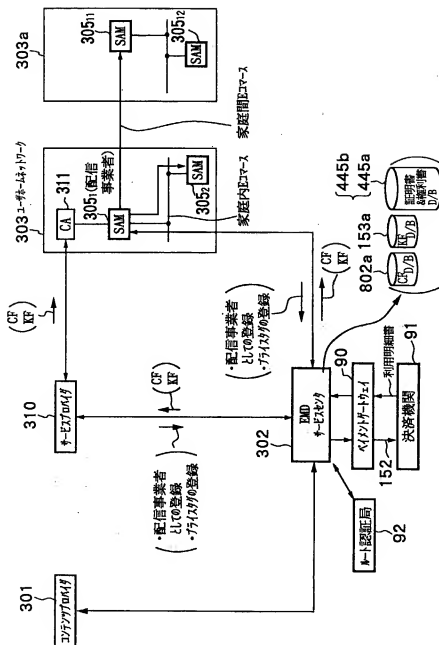


FIG.143

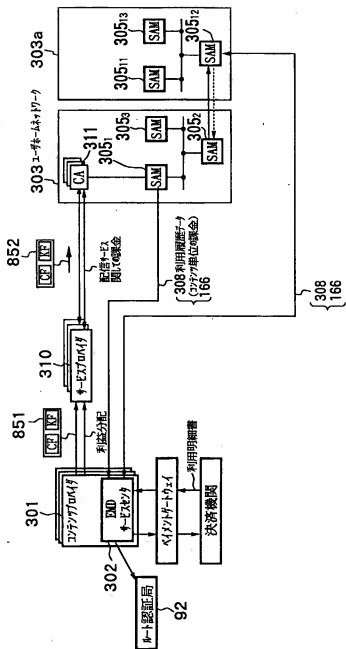


FIG.144

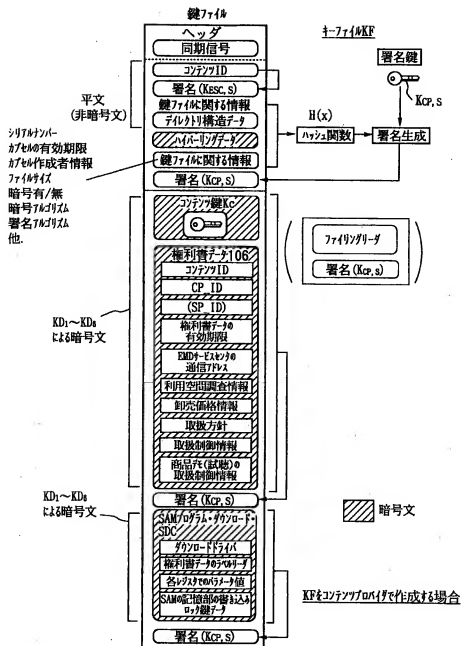
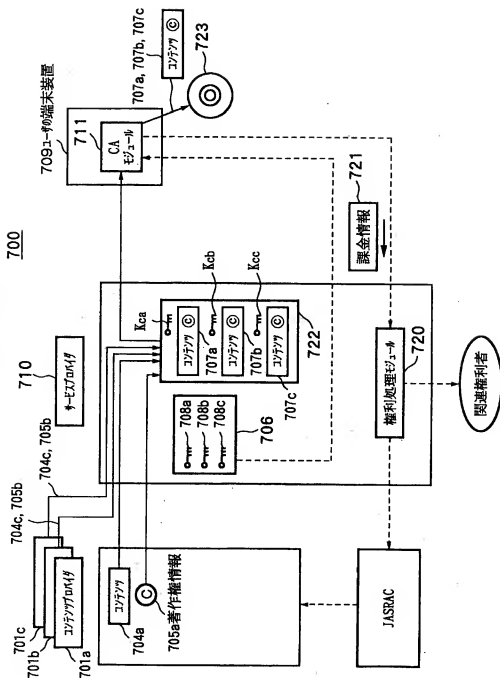


FIG.145



符号リスト

90…ペイメントゲートウェイ
91…決済機関
92…ルート認証局
100, 300…EMDシステム
101, 301…コンテンツプロバイダ
102, 302…EMDサービスセンタ
103, 303…ユーザホームネットワーク
104, 304…セキュアコンテナ
105₁～105₄, 305₁～305₄…SAM
106…権利書データ
107, 307…決済レポートデータ
108, 308…利用履歴データ
160₁…ネットワーク機器
160₂～160₄…AV機器
152, 152c, 152s…決済請求権データ
191…バス
310…サービスプロバイダ
311…CAモジュール
312…プライスタグデータ
CF…コンテンツファイル
KF…キーファイル
Kc…コンテンツ鍵データ

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06308

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ G06F15/00, G10K15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Toroku Jitsuyo Shinan Koho	1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, JICST DATA BASE contents, distribution, SuperDistribution

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Network Gata Ongaku Contents Ryutsu Platform ni kansuru Kousatsu, Multimedia, Bunsan, Kyochoto Mobile (DICOMO'98) Symposium Ronbunshu, pp.587-593, 08 July, 1998 (08.07.98) Full text	1,3,15,16,18-2 2,55,57,58,71, 74,75,77-81,91 92,143-146,14 8-151,205-208, 210,212,214,21 6,218,244,248, 249,251-254,25 8,259,261,263, 265,266,279,28 0
Y		2,4-7,9-14,17, 31,33-43,45-47 50,51,53,56,7 2,73,76,82-84. 86,87,89,109,1 10,112-139,142 147,162,163,1 65-204,209,215 246,247,250,2 56,257,260,281

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

08 February, 2001 (08.02.01)

Date of mailing of the international search report

13 February, 2001 (13.02.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06308

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A		8, 23-30, 32, 44, 48, 49, 52, 54, 59 -70, 85, 88, 90, 93-108, 111, 140 , 141, 152-161, 1 64, 211, 213, 217 , 219-243, 245, 2 55, 262, 264, 267 -278, 282-286
X	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.), 06 September, 1996 (06.09.96), pages 165 to 177, 386 to 412, 853 to 897 & JP, 10-512074, A & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	1, 3, 16, 19, 21-2 6, 29, 48, 49, 52, 54, 71, 75, 78, 80 , 81, 85, 88, 90, 1 04, 140, 141, 145 , 146, 149, 151-1 55, 160, 207, 208 , 211, 213, 242, 2 44, 245, 249, 252 , 254, 255, 259, 2 62, 264, 278-280 , 282
Y		2, 4-7, 9-14, 17, 27, 28, 31, 33-43 , 45-47, 50, 51, 5 3, 56, 72, 73, 76, 82-84, 86, 87 , 89, 105, 106, 10 8-110, 112-139, 142, 147, 156-15 9, 162, 163, 165- 204, 209, 215, 22 9, 235, 246, 247, 250, 256, 257, 26 0, 271, 274, 281, 283
A		8, 15, 18, 20, 30, 32, 44, 55, 57-70 , 74, 77, 79, 91-1 03, 107, 111, 143 , 144, 148, 150, 1 61, 164, 205, 206 , 210, 212, 214, 2 16-228, 230-234 , 236-241, 243, 2 48, 251, 253, 258 , 261, 263, 265-2 70, 272, 273, 275 -277, 284-286
Y	JP, 10-161937, A (Toshiba Corporation), 19 June, 1998 (19.06.98), Column 17, lines 1 to 19 (Family: none)	2, 7, 9, 10, 13, 27 , 28, 33-40, 105, 106, 108, 112, 11 3, 122-131, 156- 159, 163, 165-16 7, 176-181, 281, 283

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06308

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, 5701343, A (Nippon Telegraph & Telephone Corp.), 23 December, 1997 (23.12.97), Column 9, line 64 to Column 10, line 14 & JP, 8-160855, A & JP, 8-160856, A & EP, 715242, A1	2, 7, 9, 10, 13, 27 , 28, 33-40, 105, 106, 108, 112, 11 3, 122-131, 156- 159, 163, 165-16 7, 176-181, 281, 283
Y	JP, 11-85504, A (Mitsubishi Electric Corporation), 30 March, 1999 (30.03.99), Column 12, lines 26 to 31 (Family: none)	4, 9, 10, 13, 27, 2 8, 33-40, 105, 10 6, 108, 112, 113, 122-131, 156-15 9, 165-167, 176, 181, 281, 283
Y	Record Sangyo ni okeru Ongen Data base to Network Ryutsu, Research Report, Information Processing Society of Japan (IPSJ), Vol. 98, No. 85 (98-EIP-2), pp. 105-111 19 September, 1998 (19.09.98), 2. Sogo Ongaku DB Kouchiku no Kousou	229, 235, 271, 27 4
A	WO, 98/10381, A1 (Intertrust Technologies Corp.), 12 March, 1998 (12.03.98), pages 168 to 190 & JP, 2000-516743, A	1-286

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06308

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the claims of the application are divided into 18 groups: a group of inventions of claims 1-54, 71-90, 201-204, 262; a group of inventions of claims 55-61, 91-94; a group of inventions of claims 62-67, 95-100; a group of inventions of claims 68-70, 101-103; a group of inventions of claims 104-108, 245; a group of inventions of claims 109-139, 142-151, 246-254; the invention of claim 140; the invention of claim 141; a group of inventions of claims 152-161, 255; a group of inventions of claims 162-200, 205-213, 256-261, 263, 264; a group of inventions of claims 214-223, 265-268; a group of inventions of claims 224-235, 269-274; a group of inventions of claims 236-241, 275-277; a group of inventions of claims 242, 243, 278; a group of inventions of claims a group of inventions of claims 244, 279; a group of inventions of claims 280, 281; a group of inventions of claims 282, 283; and a group of inventions of claims 284-286.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl ¹ G06F15/00, G10K15/02		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl ¹ G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1926-1996年		
日本国公開実用新案公報 1971-2001年		
日本国実用新案登録公報 1996-2001年		
日本国登録実用新案公報 1994-2001年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
WPI, JICST科学技術文献データベース contents, distribution, SuperDistribution		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所に関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	ネットワーク型音楽コンテンツ流通プラットフォームに関する考察, マルチメディア, 分散, 協調とモーバイル (DICO TM 98) シンポジウム論文集, p. 587-593 8.7月. 1998 (08.07.98), 全頁を参照	1, 3, 15, 16, 18-22, 55, 57, 58, 71, 74, 75, 77-81, 91, 92, 143-146, 148- 151, 205-208, 210, 212, 214, 216, 218, 244, 248, 249, 251- 254, 258, 259,
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「I」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願		
の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 08.02.01		国際調査報告の発送日 13.02.01
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 中里 裕正 電話番号 03-3581-1101 内線 3599

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y		261, 263, 265, 266, 279, 280 2, 4-7, 9-14, 17, 31, 33-43, 45-47, 50, 51, 53, 56, 72, 73, 76, 82-84, 86, 87, 89, 109, 110, 112-139, 142, 147, 162, 163, 165-204, 209, 215, 246, 247, 250, 256, 257, 260, 281
A		8, 23-30, 32, 44, 48, 49, 52, 54, 59-70, 85, 88, 90, 93-108, 111, 140, 141, 152- 161, 164, 211, 213, 217, 219- 243, 245, 255, 262, 264, 267- 278, 282-286
X	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.) 6.9月.1996(06.09.96), 第165-177, 386-412, 853-897頁 & JP, 10-512074, A & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	1, 3, 16, 19, 21-26, 29, 48, 49, 52, 54, 71, 75, 78, 80, 81, 85, 88, 90, 104, 140, 141, 145, 146, 149, 151-155, 160, 207, 208, 211, 213, 242, 244, 245, 249, 252, 254, 255, 259, 262, 264, 278- 280, 282
Y		2, 4-7, 9-14, 17, 27, 28, 31,

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A		33-43, 45-47, 50, 51, 53, 56, 72, 73, 76, 82-84, 86, 87, 89, 105, 106, 108-110, 112- 139, 142, 147, 156-159, 162, 163, 165-204, 209, 215, 229, 235, 246, 247, 250, 256, 257, 260, 271, 274, 281, 283
		8, 15, 18, 20, 30, 32, 44, 55, 57-70, 74, 77, 79, 91-103, 107, 111, 143, 144, 148, 150, 161, 164, 205, 206, 210, 212, 214, 216-228, 230-234, 236- 241, 243, 248, 251, 253, 258, 261, 263, 265- 270, 272, 273, 275-277, 284- 286
Y	JP, 10-161937, A (株式会社東芝) 19. 6月. 1998 (19. 06. 98), 第17欄第1-19行 (ファミリーなし)	2, 7, 9, 10, 13, 27, 28, 33-40, 105, 106, 108, 112, 113, 122- 131, 156-159, 163, 165-167, 176-181, 281, 283
Y	US, 5701343, A (Nippon Telegraph & Telephone Corp.) 23. 12月. 1997 (23. 12. 97), 第9欄第64行-第10欄第14行 & JP, 8-160855, A & JP, 8-160856, A & EP, 715242, A1	2, 7, 9, 10, 13, 27, 28, 33-40, 105, 106, 108, 112, 113, 122-

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 11-85504, A (三菱電機株式会社) 30. 3月. 1999 (30. 03. 99), 第12欄第26-31行 (ファミリーなし)	131, 156-159, 163, 165-167, 176-181, 281, 283 4, 9, 10, 13, 27, 28, 33-40, 105, 106, 108, 112, 113, 122- 131, 156-159, 165-167, 176- 181, 281, 283
Y	レコード産業における音源データベースとネットワーク流通, 情報処理学会研究報告, Vol. 98, No. 85 (98-EIP-2), p. 105-111 19. 9月. 1998 (19. 09. 98), 2. 総合音楽DB構築の構想	229, 235, 271, 274
A	WO, 98/10381, A1 (Intertrust Technologies Corp.) 12. 3月. 1998 (12. 03. 98), 第168-190頁 & JP, 2000-516743, A	1-286

第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査することを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、請求の範囲1-54, 71-90, 201-204, 262/55-61, 91-94/62-67, 95-100/68-70, 101-103/104-108, 245/109-139, 142-151, 246-254/140/141/152-161, 255/162-200, 205-213, 256-261, 263, 264/214-223, 265-268/224-235, 269-274/236-241, 275-277/242, 243, 278/244, 279/280, 281/282, 283/284-286/の18群の発明に区分される。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

FIG.54

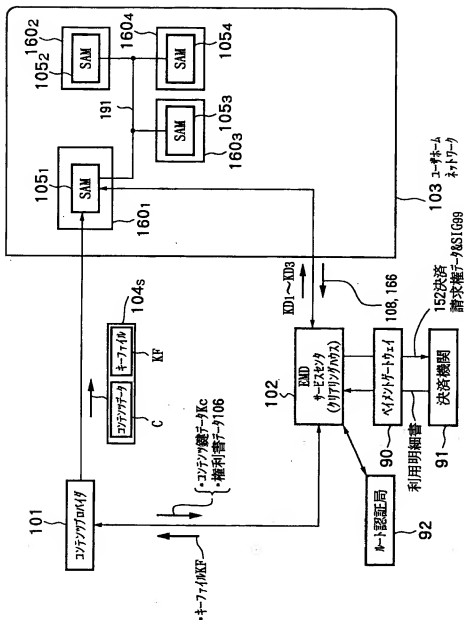


FIG.55

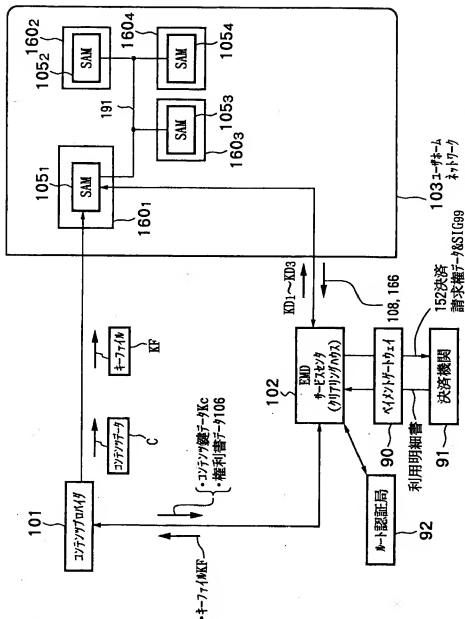


FIG.61

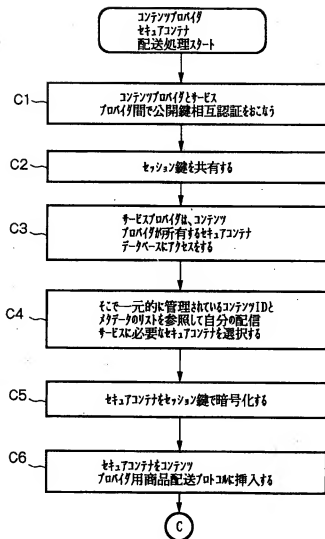


FIG.62

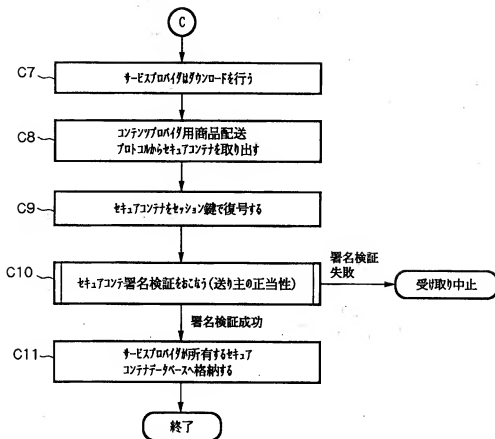
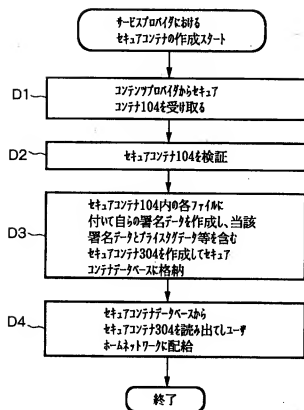


FIG.64



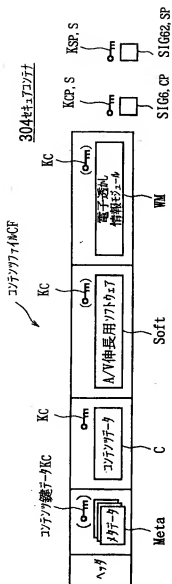


FIG. 65A

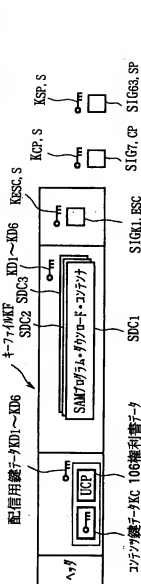


FIG. 65B

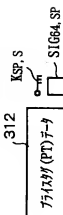


FIG. 65C

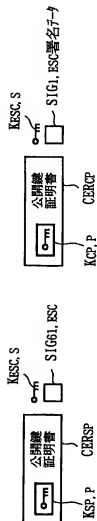


FIG. 65D

FIG.66

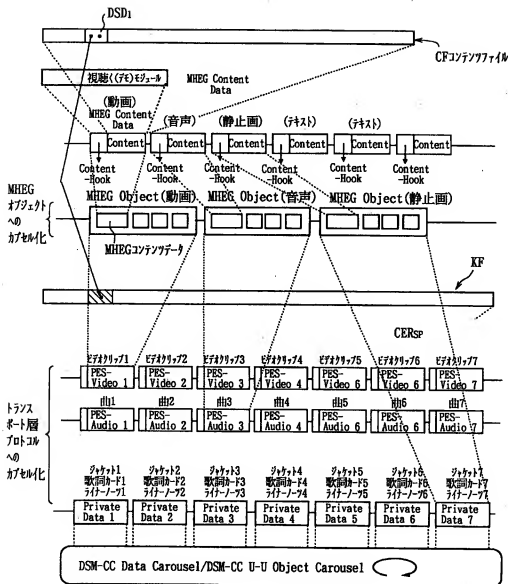


FIG.67

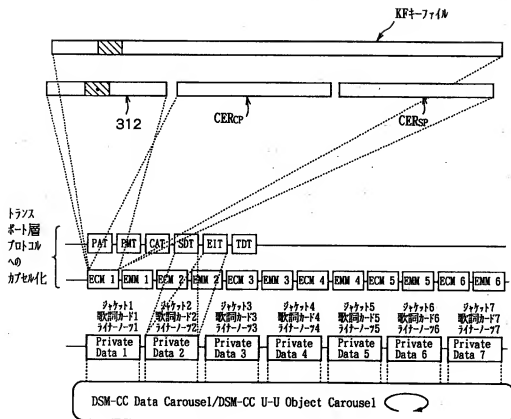


FIG.68

310システム

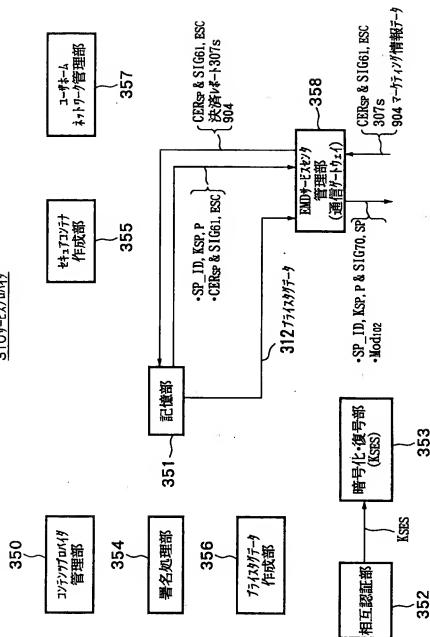


FIG.69

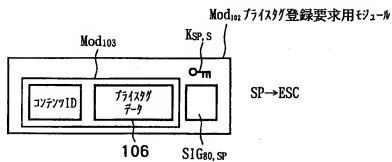


FIG.71

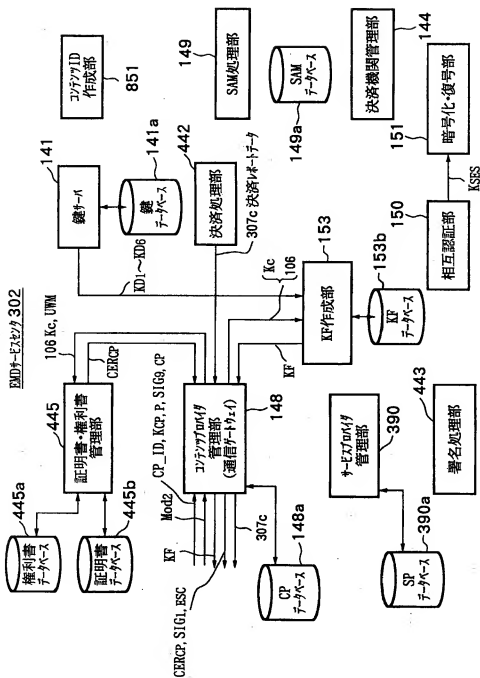


FIG.73

利用履歴テーブル308の内容

識別子Content_ID

識別子CP_ID

識別子SP_ID

コンテンツデータCの信号諸元データ

コンテンツデータCの圧縮方法

記録媒体の識別子Media_ID

識別子SAM_ID、

ユーザのUSER_ID

FIG.74

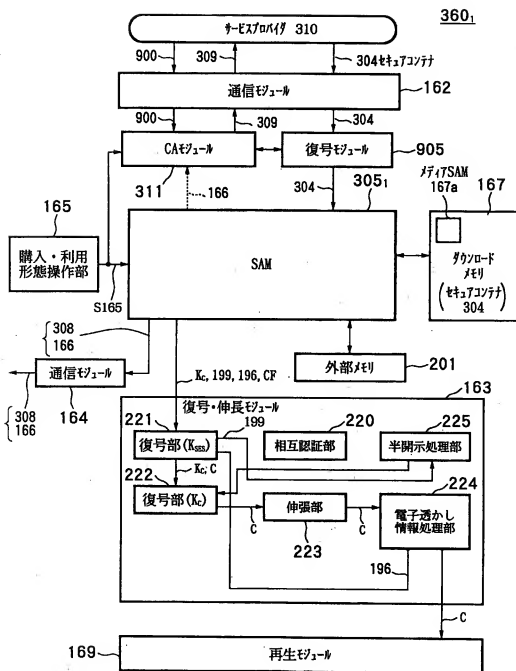


FIG.76

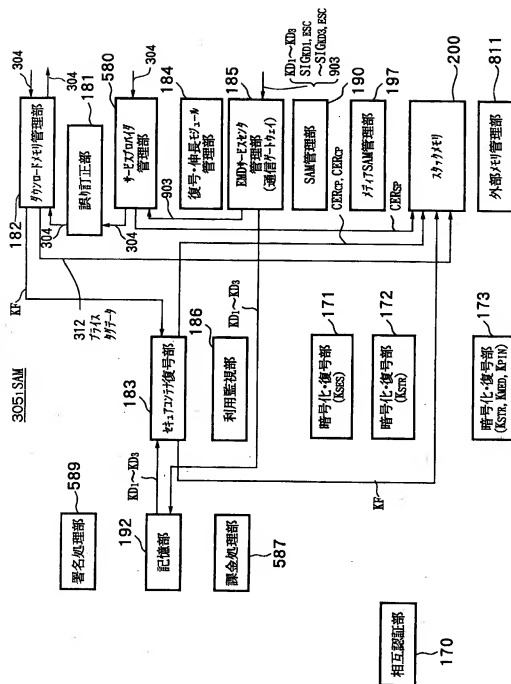


FIG.77

スタックメモリ200の記憶データ

コテンソク鍵データKc

権利書データ(UCP)106

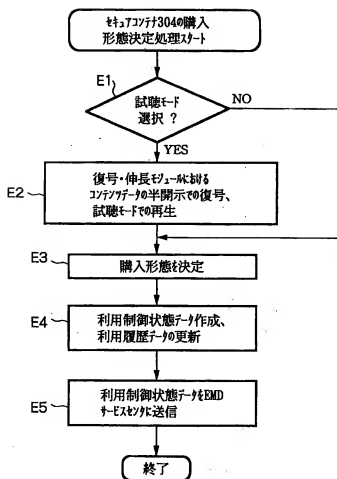
不揮発性メモリ201のロック鍵データK_{Loc}コテンソクプロバイダ301の公開鍵証明書データCER_{CP}サービスプロバイダ301の公開鍵証明書データCER_{SP}

利用制御状態データ(UCS)166

SAMプログラム・ダウンロード・コンテナSD₁〜SD₃

プレイスタデータ312

FIG.79



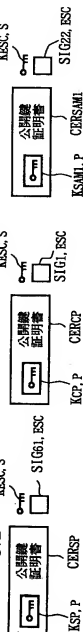
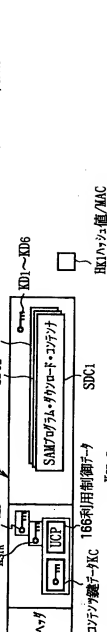
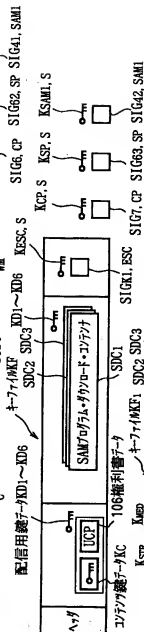
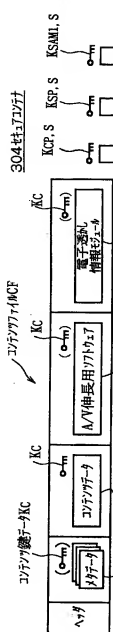


FIG.82

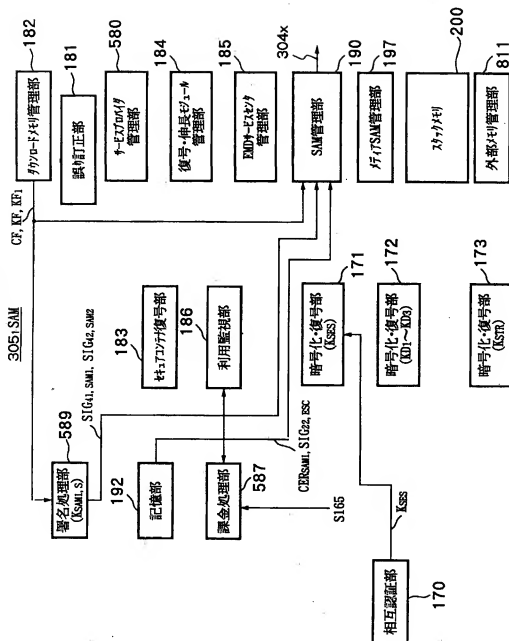


FIG.83

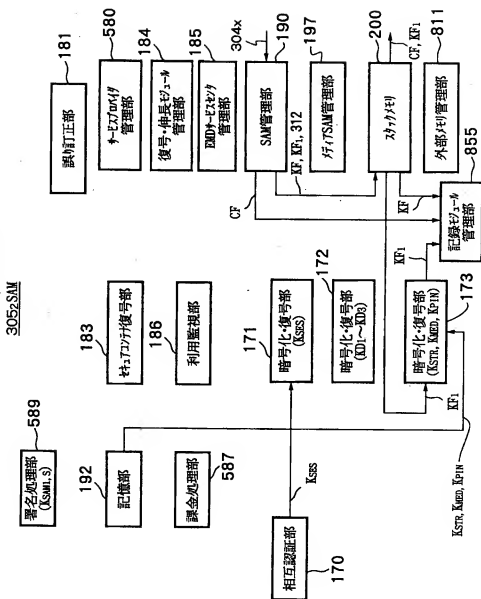


FIG.84

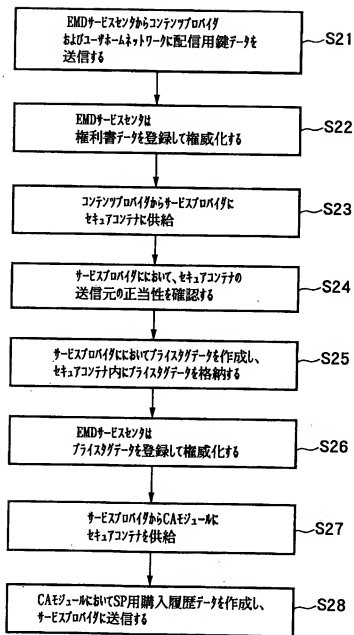


FIG.85

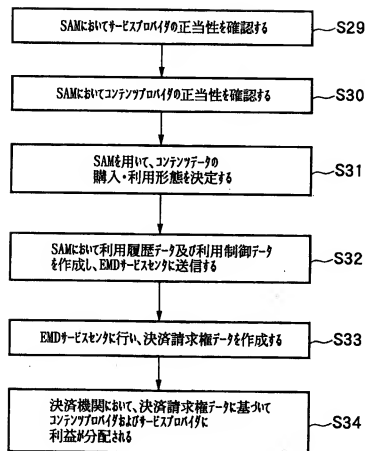


FIG.88

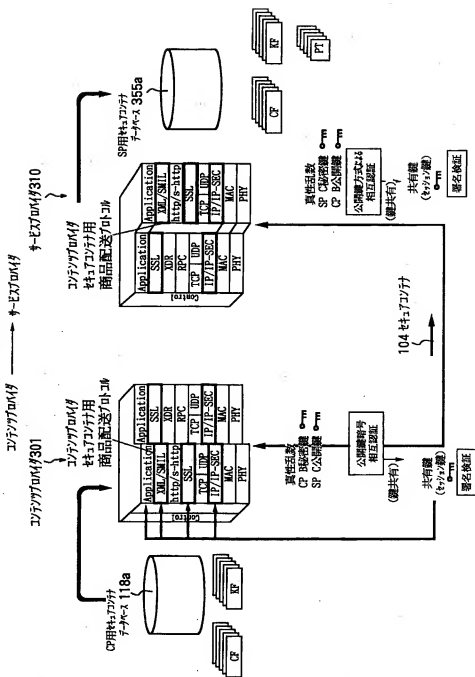


FIG.90

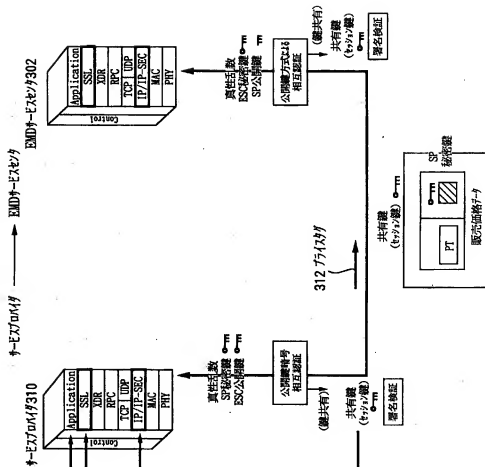


FIG.91

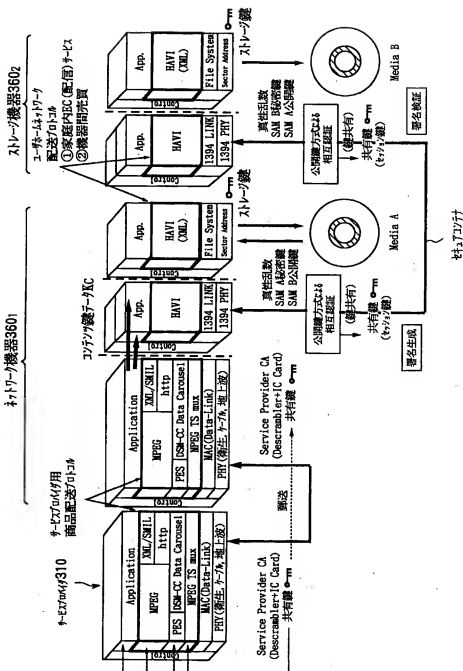


FIG.92

デジタル放送方式XML/SMIL/BMLを利用した場合の
701.54層層への付加位置関係

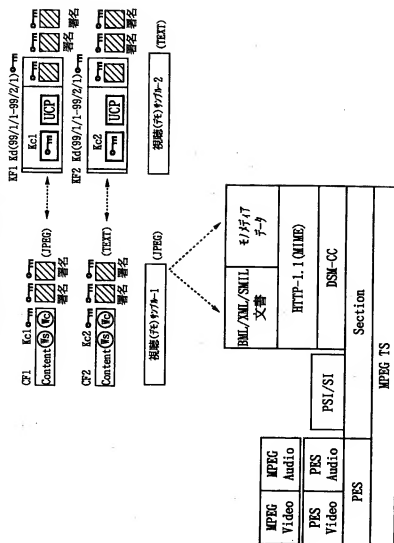


FIG.93

右の放送方式でMPEGを利用した場合の
付随情報の付加方法

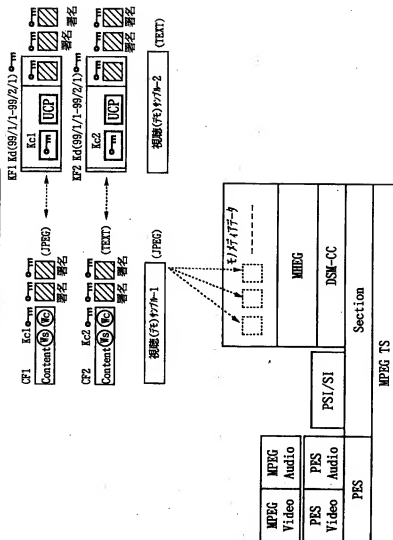


FIG.94

インターネットのデータ伝送方式XML/SMTP
プロトコル層の構成例

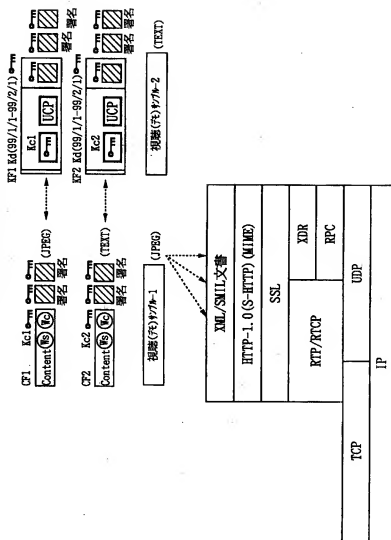


FIG.97

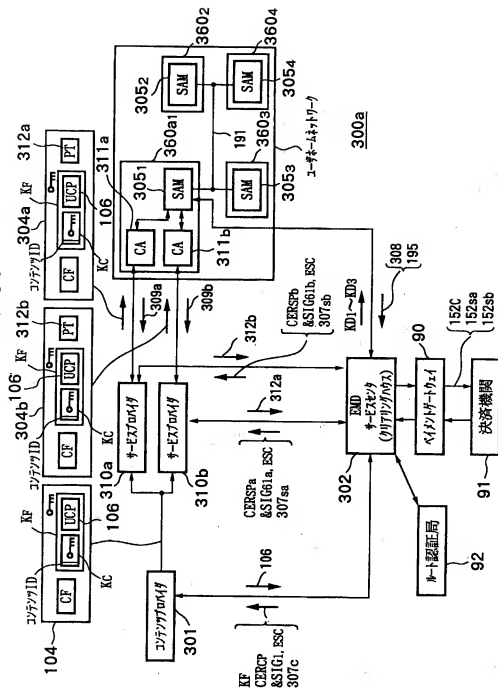


FIG.98

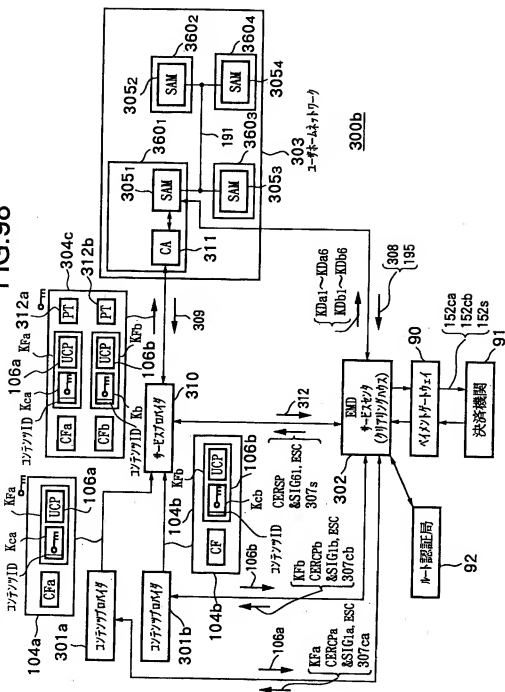
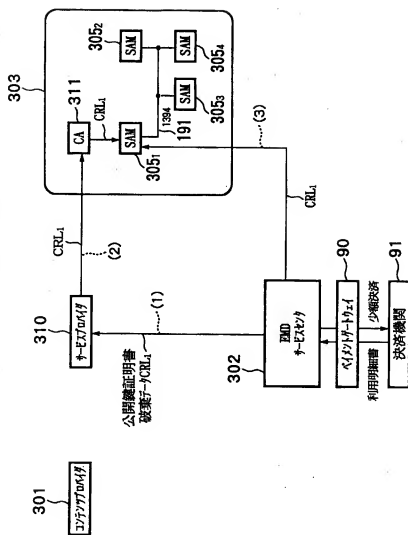
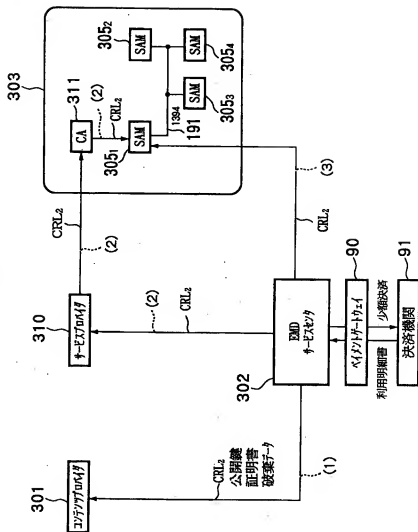


FIG.102



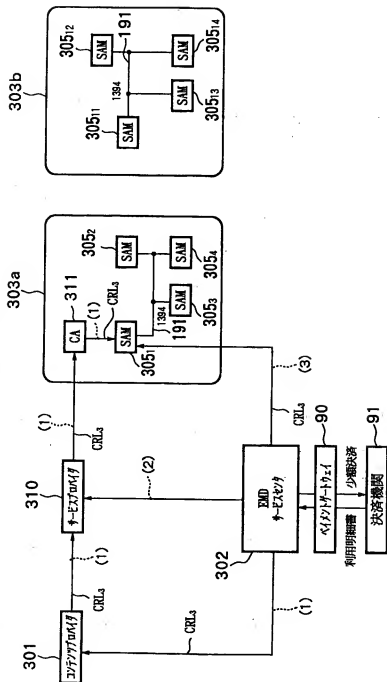
CRLが有効な場合

FIG.103



CRL2が無効な場合

FIG. 104



CERSAM2を無効にする場合

当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

260. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前

記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

261. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供方法。

262. データ提供装置からデータ処理装置にコンテンツデータを配給し、管

理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

263. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと

前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供方法。

264. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

265. データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理

装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

266. データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納し

たキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

267. データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコン

テンツデータの取り扱いを決定する

データ提供方法。

268. データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

269. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

270. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納さ

れた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

271. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

272. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提

供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

273. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プ

ロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

274. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

275. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベ

ース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

276. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マス

ソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

277. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスターソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成

し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

278. データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテン

ツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る

データ提供方法。

279. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータを提供し、

前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する

データ提供方法。

280. データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

281. 前記データ提供装置は、自らの署名データを当該署名データの作成方式に依存しない形式でさらに格納した前記モジュールを前記データ処理装置に配給する

請求項280に記載のデータ提供システム。

282. データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

283. 前記データ提供装置は、自らの署名データを当該署名データの作成方式に依存しない形式でさらに格納した前記第1のモジュールを前記データ配給装

置に提供する

請求項 282 に記載のデータ提供システム。

284. データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した複数の第2のモジュールを、前記データ処理装置との間の相互認証によって得られた共有鍵を用いて暗号化した後に、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記複数の第2のモジュールを前記共有鍵を用いて復号し、当該復号した前記複数の第2のモジュールの中から単数または複数の第2のモジュールを選択し、前記第2のモジュールの配給サービスに対しての課金処理を行う第1の処理回路と、前記選択された前記第2のモジュールを受けて当該第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する耐タンパ性の第2の処理回路とを有する

データ提供システム。

285. 前記第1の処理回路は、前記データ配給装置の前記第2のモジュールの配給サービスに関してのデータ配給装置用履歴データを作成し、当該データ配給装置用履歴データを前記データ配給装置に送り、

前記データ配給装置は、前記データ配給装置用履歴データに基づいて

課金処理を行う

請求項 2 8 4 に記載のデータ提供システム。

2 8 6. 前記データ提供装置、前記データ配給装置および前記データ処理装置を管理する管理装置をさらに有し、

前記第 2 の処理回路は、前記コンテンツデータの取り扱いを決定し、当該決定に応じた利用履歴データを作成し、当該利用履歴データを前記管理装置に送り、

前記管理装置は、前記利用履歴データに基づいて、前記データ処理装置の関係者が支払った前記コンテンツデータに関しての利益を前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行う

請求項 2 8 4 に記載のデータ提供システム。

FIG.1

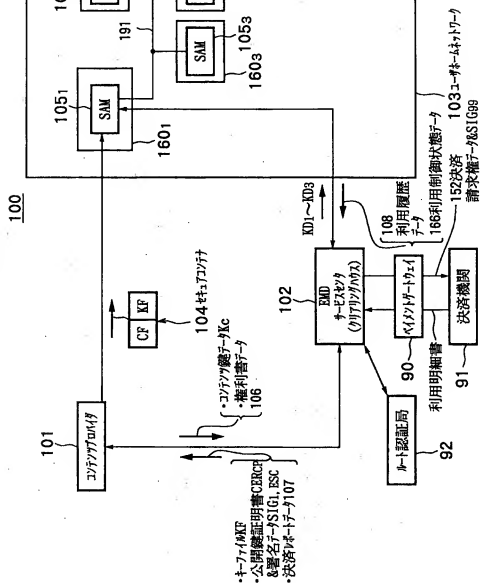


FIG.2

本発明の権利管理の概念

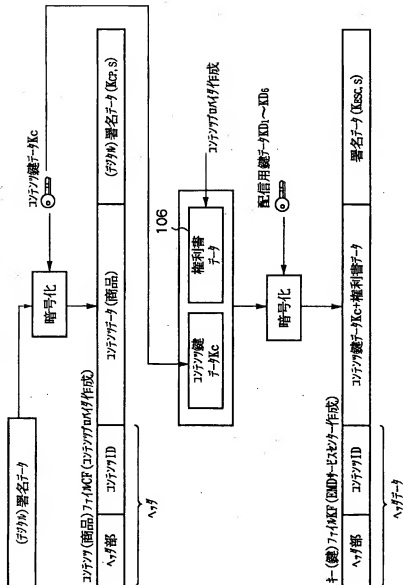


FIG.3

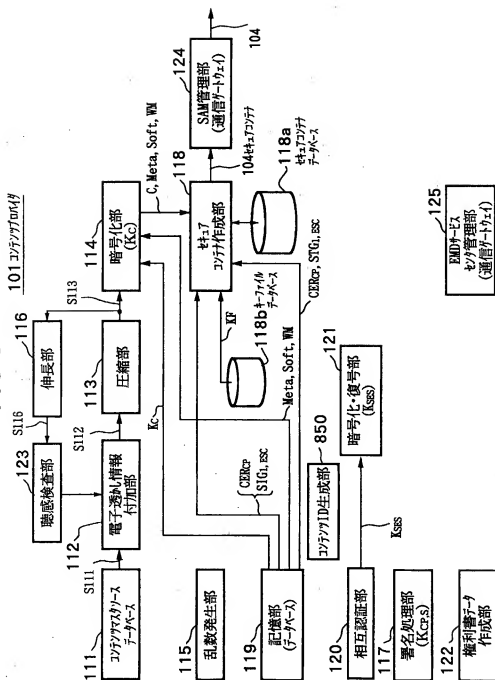
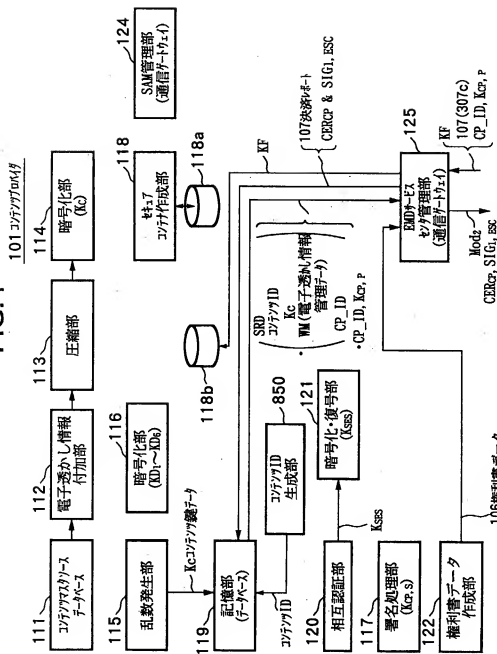


FIG.4



104 柱 570 ヲ

コテンツァイMCF

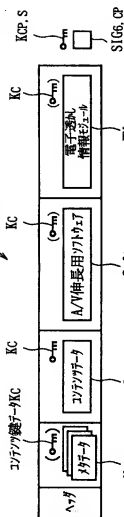


FIG. 5A

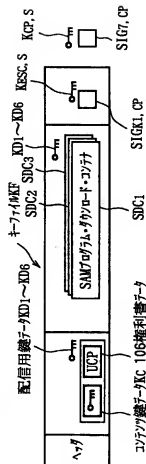


FIG. 5B

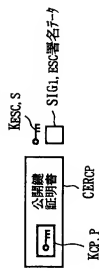


FIG. 5C

FIG.6

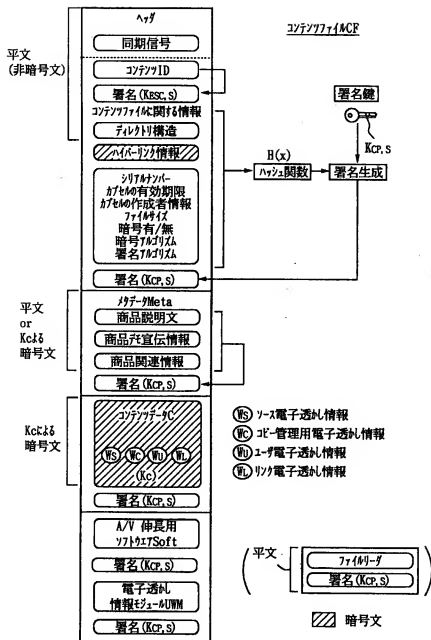


FIG.7

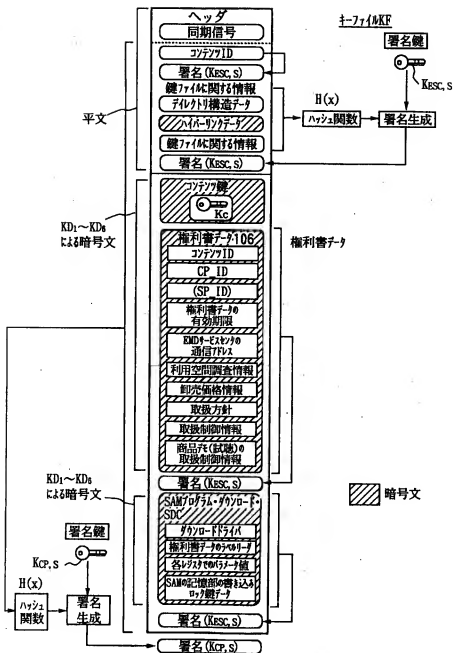


FIG.8

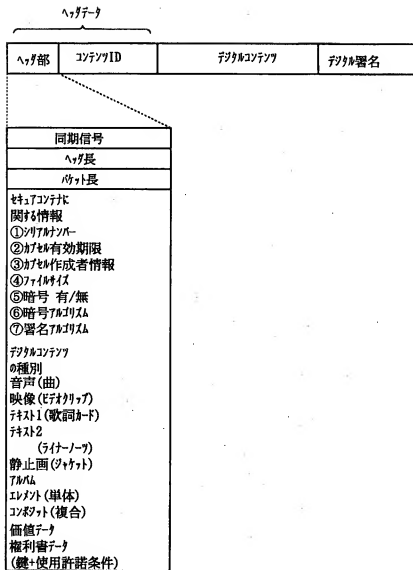


FIG.9

コンテンツIDの基本構造

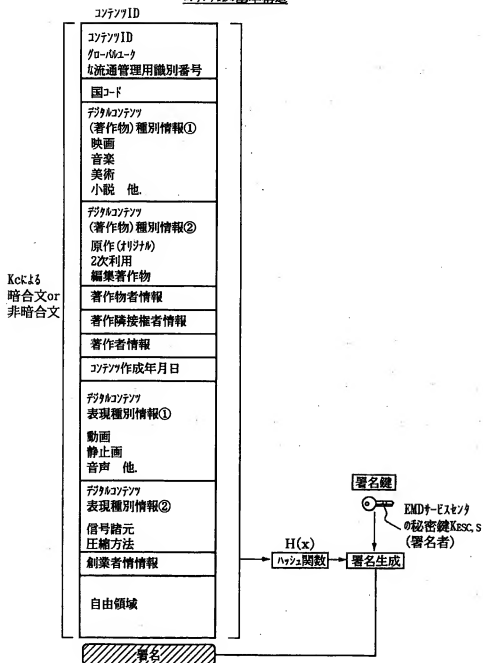


FIG.10

セクタコンテナのディレトリ構造

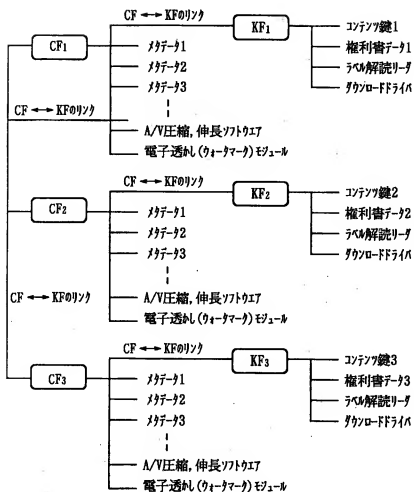


FIG.11

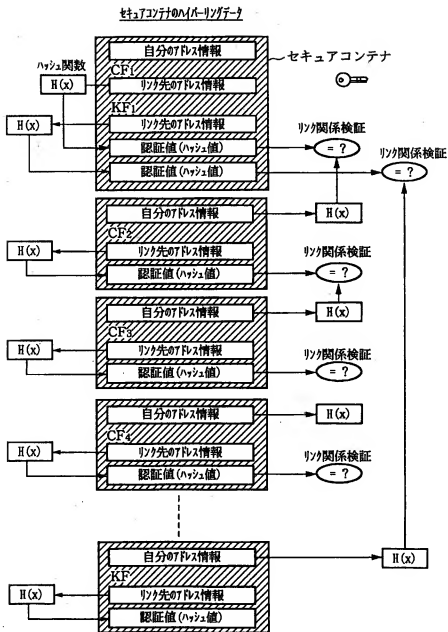


FIG.12

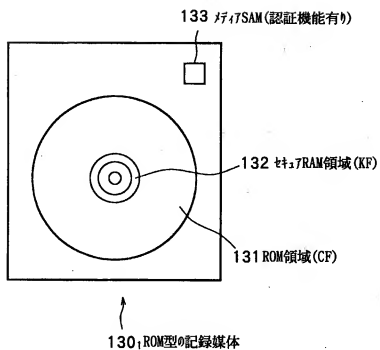


FIG.13

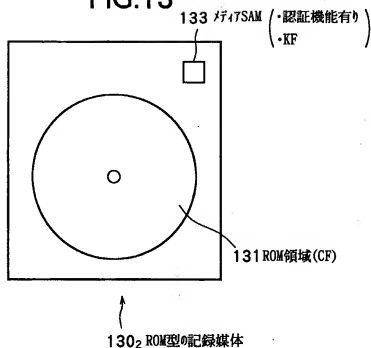


FIG.14

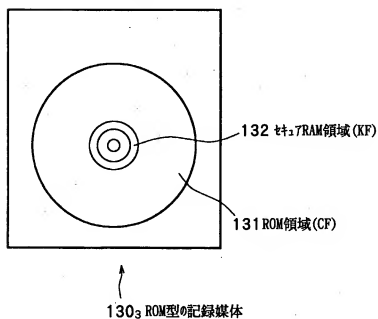


FIG.15

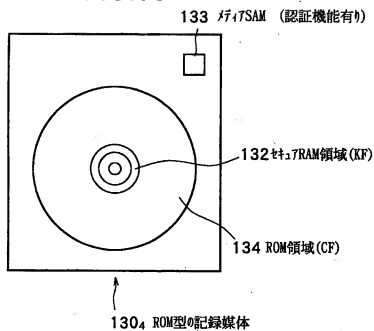


FIG.16

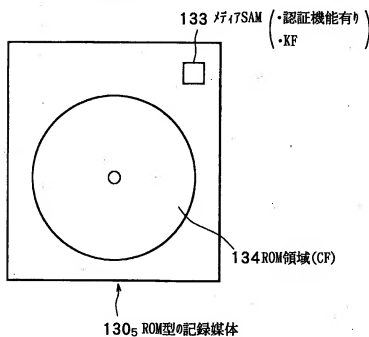


FIG.17

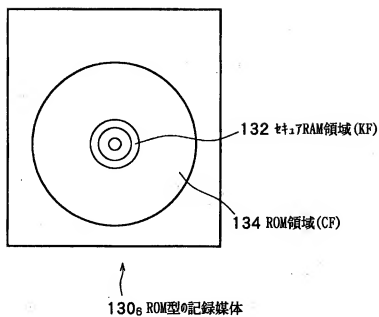


FIG.18

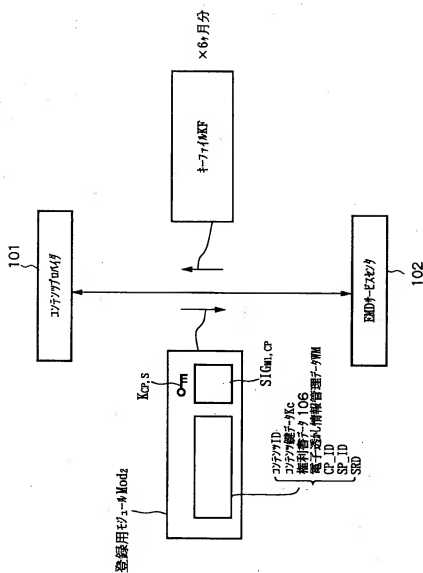


FIG.19

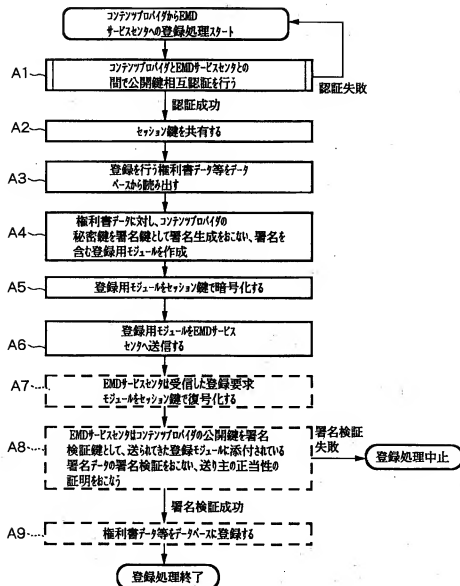


FIG.21

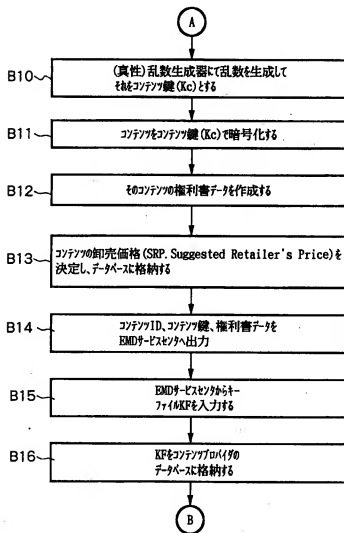


FIG.22

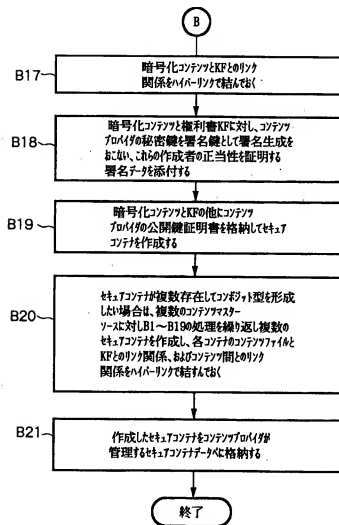


FIG. 23

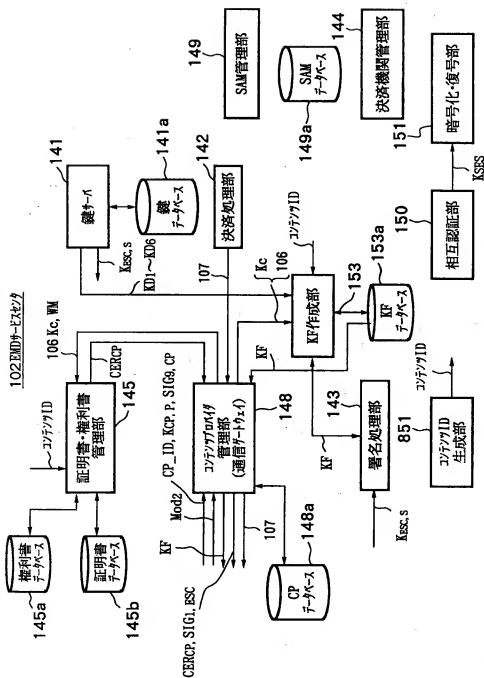


FIG.24

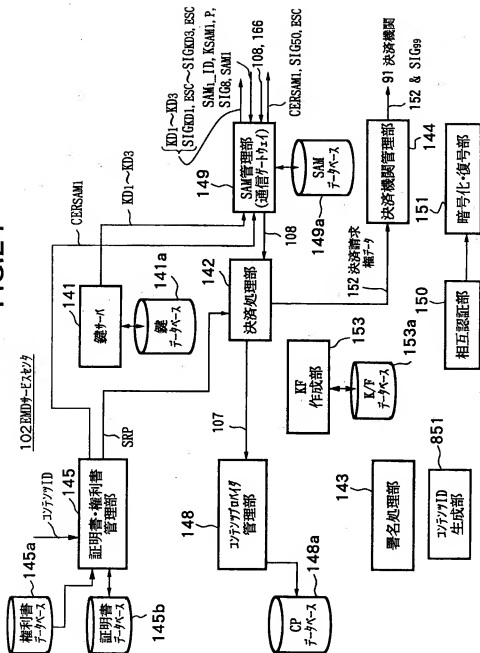


FIG.25

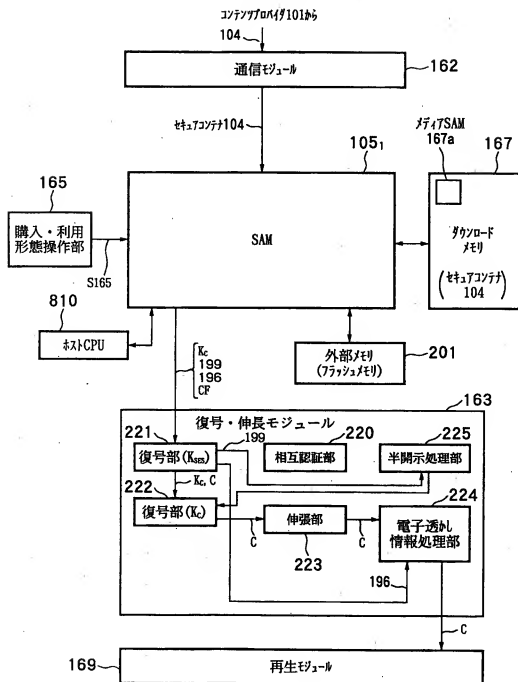


FIG.26

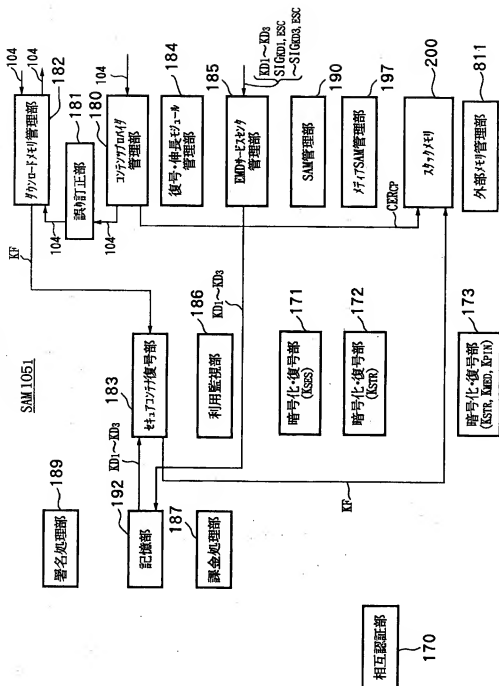


FIG.27

外部メモリ201に記憶されるデータ

利用履歴データ108
SAM登録リスト

FIG.28

スタックメモリ200に記憶されるデータ

コンテナ鍵データKc
権利書データ(UCP) 106
記憶部(フラッシュメモリ) 192のロック鍵データK_{Loc}
コンテナプロバイダ101の公開鍵証明書CER_{CP}
利用制御状態データ(UCS) 166
SAMプログラム・ダウンロード・コンテナSD₁〜SD₃

FIG.29

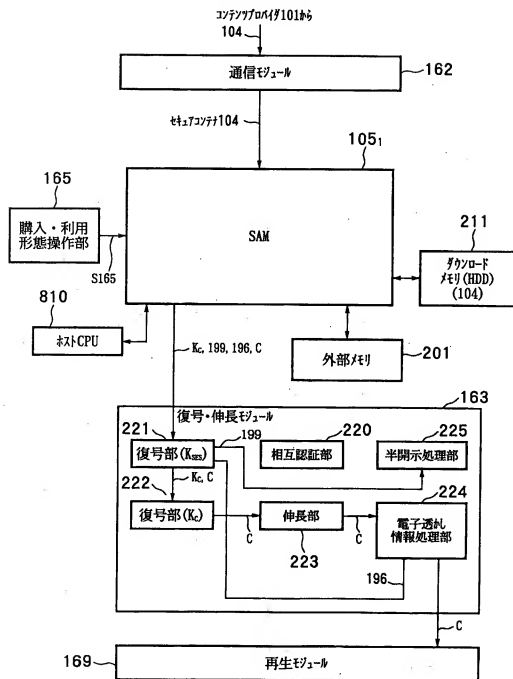


FIG.30

記憶部192に記憶されるデータ

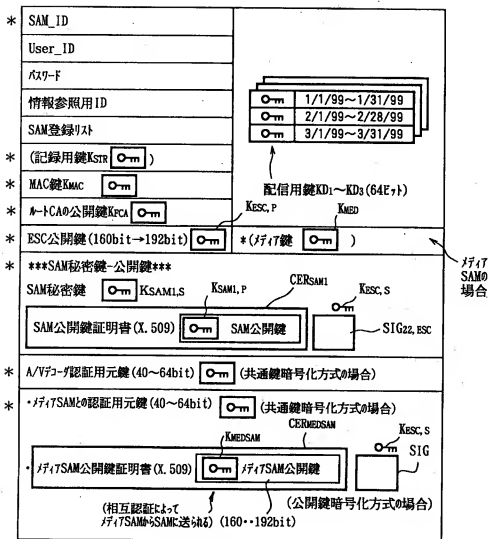
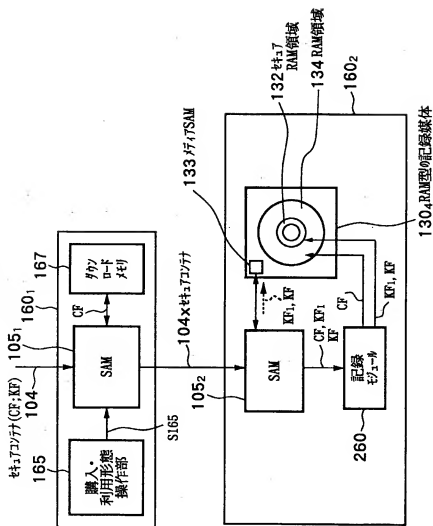


FIG.32



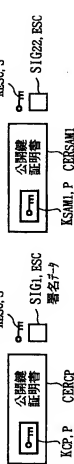
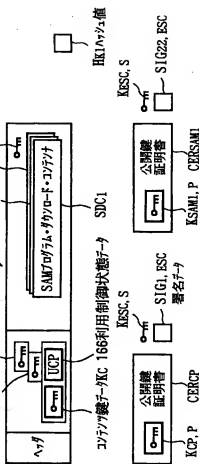
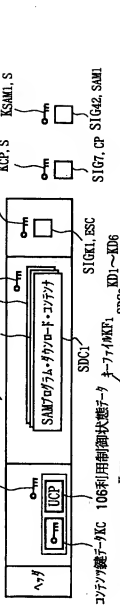
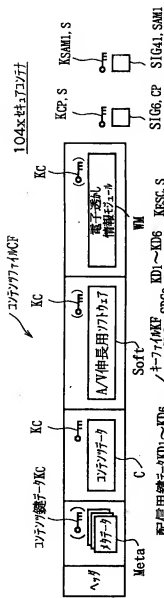


FIG.36

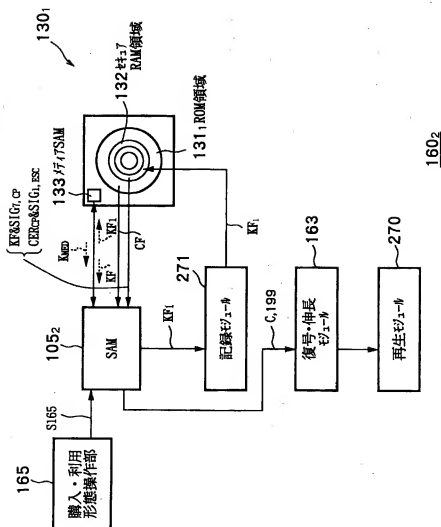


FIG.38

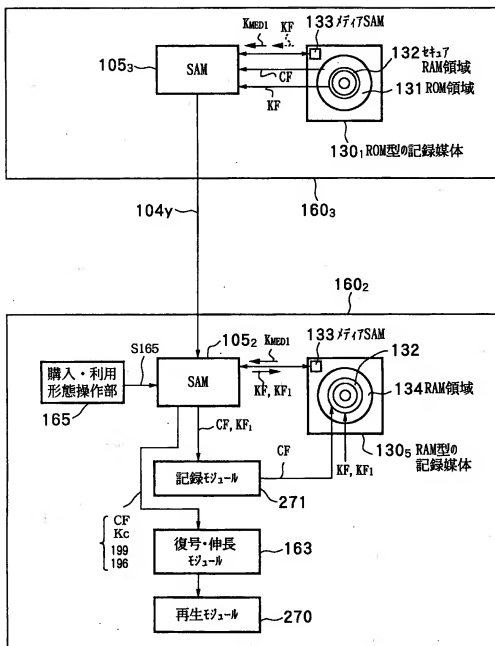
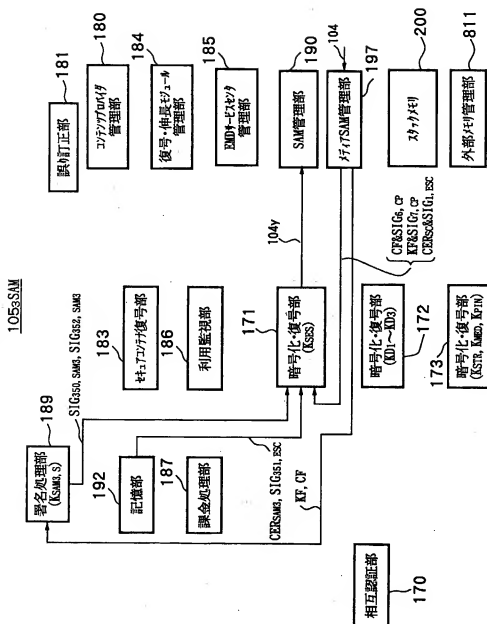


FIG.39



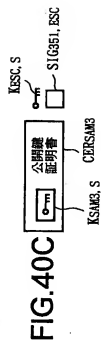
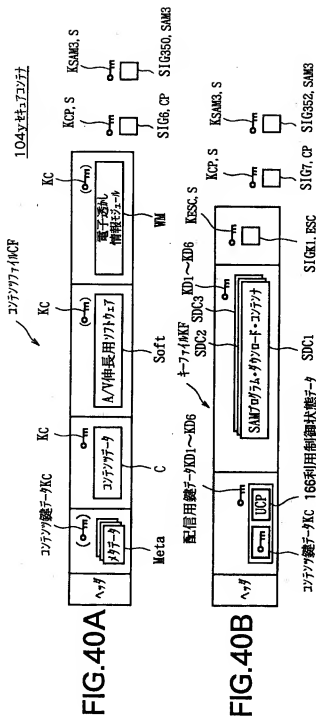
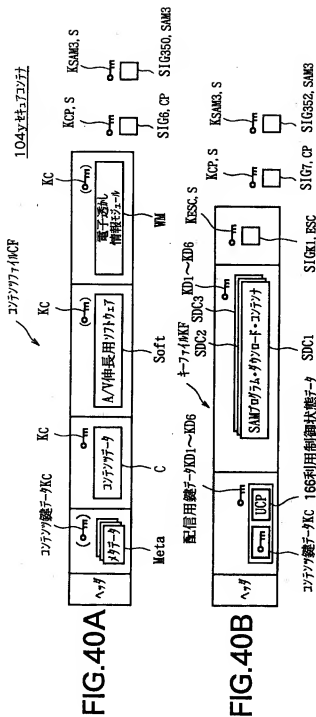


FIG.41

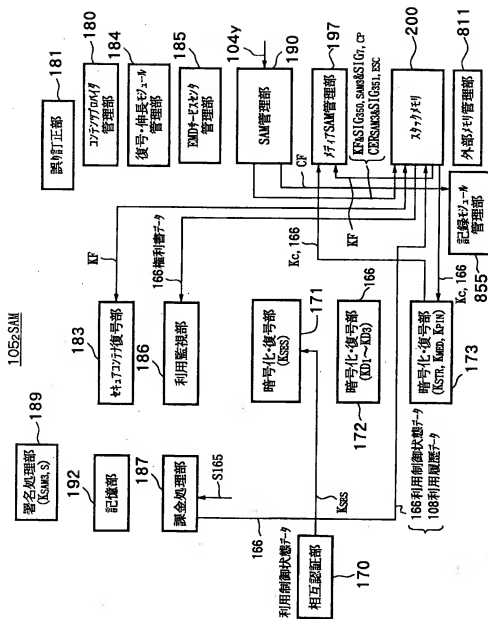


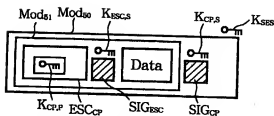
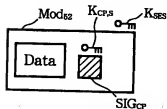
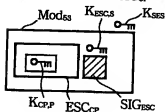
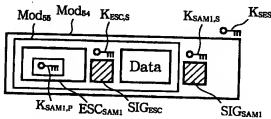
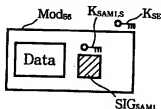
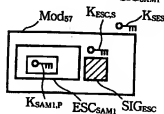
FIG.42A 101 (CP) → SAM105₁
(イソ・パツフ)FIG.42B 101 (CP) → SAM105₁
(79ト・パツ・パツフ)FIG.42C 102 (ESC) → SAM105₁
(79ト・パツ・パツフ)FIG.42D SAM105₁ → 101 (CP)
(イソ・パツフ)FIG.42E SAM105₁ → 101 (CP)
(79ト・パツ・パツフ)FIG.42F 102 (ESC) → 101 (CP)
(79ト・パツ・パツフ)

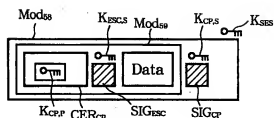
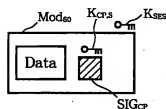
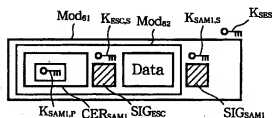
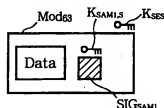
FIG.43G 101 (CP) → 102 (ESC)
(17バイト)FIG.43H 101 (CP) → 102 (ESC)
(7バイト)FIG.43I SAM1051 → 102 (ESC)
(17バイト)FIG.43J SAM1051 → 102 (ESC)
(7バイト)

FIG.44

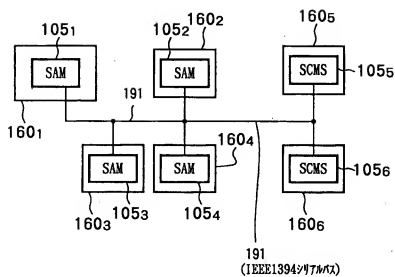


FIG.45

SAM登録リスト (SAM Registration List) (SAM作成)

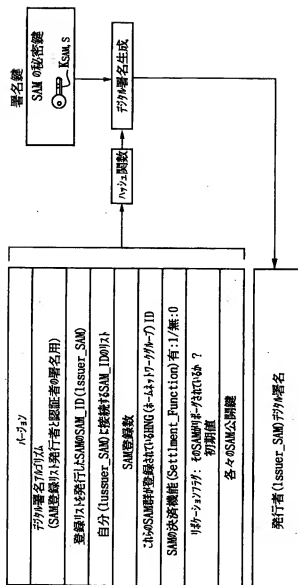


FIG.46

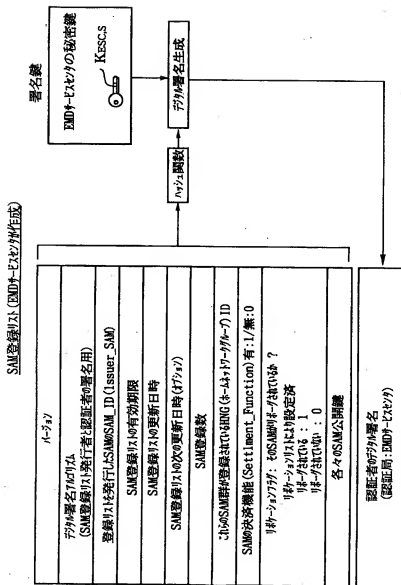


FIG.47

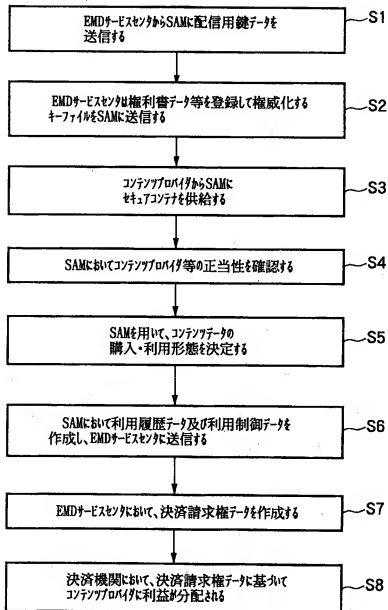


FIG.49

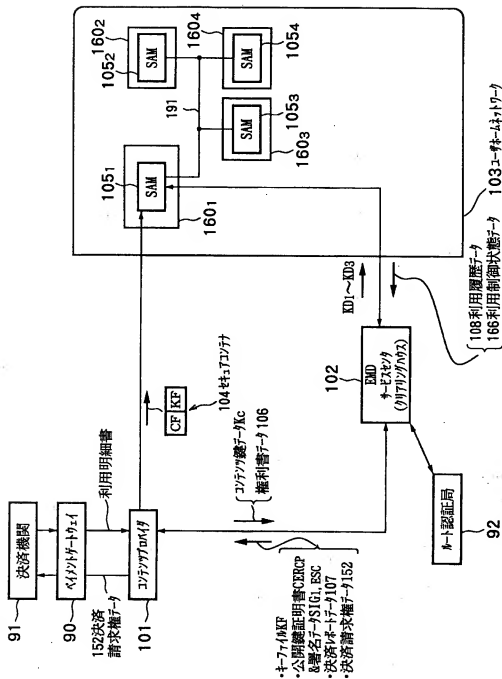


FIG.50

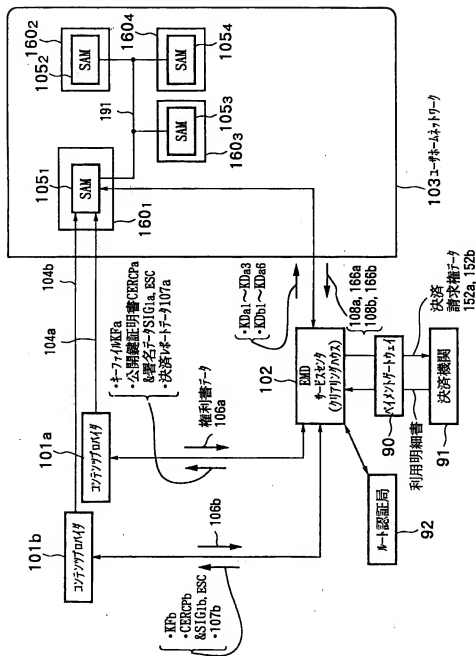
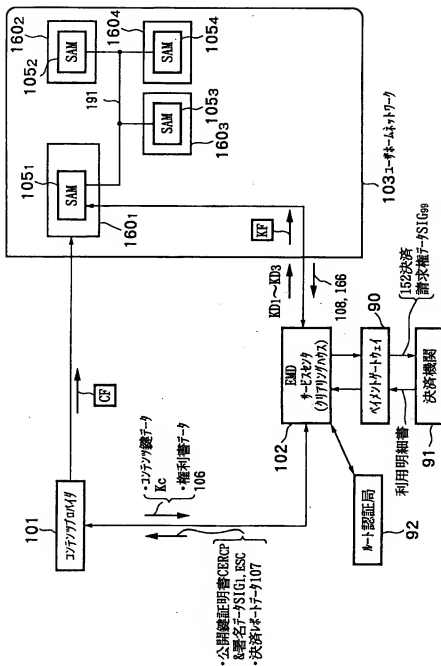


FIG.52



ツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

100. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

101. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

102. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツ

データについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルに対応する前記データ配給装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

103. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納さ

れた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

104. データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

105. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記モジュールを前記データ処理装置に配給する

請求項104に記載のデータ提供システム。

106. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて、当該データが改竄されていないかを検証するためのデータと、当該データを所定の機関によって正規に認証されているかを検証するための署名データとのうち少なくとも一方のデータをさらに格納した前記モジュールを前記データ処理装置に配給する

請求項104に記載のデータ提供システム。

107. 前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態を決定し、

前記コンテンツデータを他のデータ処理装置に転送する場合に、当該コンテンツデータの購入者の正当性を示す署名データと、当該コンテンツデータの送信者の正当性を示す署名データとを異ならせる

請求項104に記載のデータ提供システム。

108. 前記データ提供装置は、当該データ提供装置の秘密鍵データおよびハッシュ関数を用いて前記署名データを作成する

請求項104に記載のデータ提供システム。

109. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

110. 前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作

成する

請求項 109 に記載のデータ提供システム。

111. 前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する

請求項 109 に記載のデータ提供システム。

112. 前記データ提供装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記モジュールを前記データ処理装置に配給する

請求項 110 に記載のデータ提供システム。

113. 前記データ処理装置は、前記モジュールに格納された前記署名データを検証して、前記コンテンツファイルの作成者および配給者と、前記キーファイルの作成者および配給者との正当性のうち少なくとも一つを確認する

請求項 112 に記載のデータ提供システム。

114. 前記データ提供装置は、前記コンテンツデータが圧縮されている場合に、当該コンテンツデータを伸長する伸長用ソフトウェアを前記コンテンツファイルにさらに格納する

請求項 109 に記載のデータ提供システム。

115. 前記データ提供装置は、前記コンテンツファイルに電子透かし情報が埋め込まれている場合に、当該電子透かし情報を検出するのに用いられる情報を含む電子透かし情報モジュールを前記コンテンツファイルにさらに格納する

請求項 109 に記載のデータ提供システム。

116. 前記データ提供装置は、前記コンテンツデータの内容の説明に関する

メタデータを前記コンテンツファイルに格納して、あるいは前記コンテンツファイルとは別に前記データ処理装置に配給する

請求項 109 に記載のデータ提供システム。

117. 前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、

前記配信用鍵データを前記データ処理装置に配給する

請求項 109 に記載のデータ提供システム。

118. 前記管理装置および前記データ処理装置は、有効期間が規定された複数の配信用鍵データを有し、対応する期間の前記配信用鍵データを用いる

請求項 117 に記載のデータ提供システム。

119. 前記管理装置は、前記権利書データの文法を記述したデータをさらに格納した前記キーファイルを作成する

請求項 109 に記載のデータ提供システム。

120. 前記管理装置は、前記コンテンツファイルおよび前記キーファイルを読み込むための情報を示すデータであるファイルリーダを前記データ処理装置に配給し、

前記データ処理装置は、前記ファイルリーダに基づいて、前記コンテンツファイルおよび前記キーファイルの読み込みを行う

請求項 109 に記載のデータ提供システム。

121. 前記データ提供装置は、前記コンテンツファイルおよび前記キーファイルを読み込むための情報を示すデータであるファイルリーダをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記ファイルリーダに基づいて、前記コンテンツファイルおよび前記キーファイルの読み込みを行う

請求項 109 に記載のデータ提供システム。

122. 前記データ提供装置は、自らの秘密鍵データを用いて前記署名データ

を作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する

請求項 1 1 3 に記載のデータ提供システム。

1 2 3. 前記データ提供装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 1 2 2 に記載のデータ提供システム。

1 2 4. 前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 1 2 2 に記載のデータ提供システム。

1 2 5. 前記データ提供装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項 1 2 2 に記載のデータ提供システム。

1 2 6. 前記データ提供装置は、前記モジュールを記録した記録媒体を作成する

請求項 1 2 2 に記載のデータ提供システム。

1 2 7. 前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項 1 2 2 に記載のデータ提供システム。

1 2 8. 前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗

号化されたコンテンツデータとを復号装置に出力する

請求項 1 2 2 に記載のデータ提供システム。

1 2 9. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項 1 2 9 に記載のデータ提供システム。

1 3 0. 前記管理装置は、コンテンツデータ単位で、前記利益分配処理を行う

請求項 1 2 9 に記載のデータ提供システム。

1 3 1. 前記データ提供装置は、複数の前記コンテンツファイルと、当該複数のコンテンツファイルにそれぞれ対応する複数のキーファイルとを格納したモジュールを前記データ処理装置に配給し、

前記コンテンツファイルには、前記複数のコンテンツファイル相互間の関係と、前記キーファイルとの関係とを示すディレクトリ構造データが含まれている

請求項 1 2 9 に記載のデータ提供システム。

1 3 2. 前記データ提供装置は、前記モジュールを格納する記憶回路

をさらに有する請求項 1 0 9 に記載のデータ提供システム。

1 3 3. 前記データ提供装置は、前記コンテンツデータに固有に割り付けられたコンテンツ識別子に基づいて、前記モジュールを管理する

請求項 1 3 2 に記載のデータ提供システム。

1 3 4. 前記管理装置は、前記コンテンツ識別子をさらに格納した前記キーフ

ファイルを作成する

請求項 1 3 3 に記載のデータ提供システム。

1 3 5. 前記コンテンツ識別子は、前記データ提供装置が前記記憶回路に格納するコンテンツデータ内でユニークに決められている

請求項 1 3 3 に記載のデータ提供システム。

1 3 6. 前記コンテンツ識別子は、前記グローバルユニークに決められている

請求項 1 3 3 に記載のデータ提供システム。

1 3 7. 前記データ提供装置は、前記コンテンツ識別子を生成する

請求項 1 3 3 に記載のデータ提供システム。

1 3 8. 前記データ提供装置は、前記モジュールを格納する記憶回路

をさらに有する請求項 1 3 3 に記載のデータ提供システム。

1 3 9. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを有する

請求項 1 3 3 に記載のデータ提供システム。

1 4 0. 管理装置によって管理され、データ処理装置にコンテンツデータを配給するデータ提供装置において、

暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを前記管理装置から受け、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給する

データ提供装置。

1 4 1. 管理装置によって管理され、コンテンツデータを利用するデータ処理

装置において、

暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルと、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルとを含むモジュールを受け、

前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信する

データ処理装置。

142. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

143. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ

提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

144. 前記データ提供装置は、複数の前記コンテンツファイルと、当該複数のコンテンツファイルにそれぞれ対応する複数のキーファイルとを個別に前記データ処理装置に配給し、

前記コンテンツファイルおよび前記キーファイルには、相互間の対応関係を示すハイパーリンク情報が含まれている

請求項143に記載のデータ提供システム。

145. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化され

たコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

146. 前記データ提供装置は、複数の前記コンテンツファイルを前記データ処理装置に配給し、

前記管理装置は、前記複数のコンテンツファイルをそれぞれ対応する複数のキーファイルを前記データ処理装置に配給し、

前記コンテンツファイルおよび前記キーファイルには、相互間の対応関係を示すハイパーリンク情報が含まれている

請求項145に記載のデータ提供システム。

147. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納され

た前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

148. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

149. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依

存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

150. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

151. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理

装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

152. データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

153. 前記データ配給装置は、前記提供を受けた第1のモジュールを包括させた前記第2のモジュールを作成し、当該作成した第2のモジュールを前記データ処理装置に配給する

請求項 152 に記載のデータ提供システム。

154. 前記データ配給装置は、前記コンテンツデータの価格を示す価格データをさらに格納した前記第2のモジュールを前記データ処理装置に配給する

請求項 152 に記載のデータ提供システム。

155. 前記データ配給装置は、前記データ提供装置が前記コンテンツデータについて決定した卸売価格に基づいて、前記価格データを決定する

請求項 154 に記載のデータ提供システム。

156. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第1のモジュールを前記データ配給装置に提供する

請求項 152 に記載のデータ提供システム。

157. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて、当該データが改竄されていないかを検証するためのデータと、当該データを所定の機関によって正規に認証されているかを検証するための署名データとのうち少なくとも一方のデータをさらに格納した前記第1のモジュールを前記データ配給装置に提供する

請求項 156 に記載のデータ提供システム。

158. 前記データ配給装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第2のモジュールを前記データ処理装置に提供する

請求項 152 に記載のデータ提供システム。

159. 前記データ配給装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて、当該データ

タが改竄されていないかを検証するためのデータと、当該データを所定の機関によって正規に認証されているかを検証するための署名データとのうち少なくとも一方のデータをさらに格納した前記第2のモジュールを前記データ処理装置に提供する

請求項152に記載のデータ提供システム。

160. 管理装置をさらに有し、

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項152に記載のデータ提供システム。

161. 前記データ処理装置は、前記データ配給装置の前記配給に関する配給履歴データを前記データ配給装置に送信し、

前記データ配給装置は、前記配給履歴データに基づいて、前記配給に関する課金処理を行う

請求項152に記載のデータ提供システム。

162. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを

作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

163. 前記管理装置は、前記キーファイルの作成者の正当性を検証するため署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する

請求項162に記載のデータ提供システム。

164. 前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、前記受信した前記コンテンツ鍵データおよび前記権利書データを登録する

請求項162に記載のデータ提供システム。

165. 前記データ提供装置は、前記コンテンツファイルの作成者および提供者と、前記キーファイルの提供者との正当性のうち少なくとも一つを検証するた

めの署名データをそれぞれ作成し、当該署名データをさらに格納した前記第1のモジュールを前記データ処理装置に配給する

請求項162に記載のデータ提供システム。

166. 前記データ配給装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第2のモジュールを前記データ処理装置に配給する

請求項162に記載のデータ提供システム。

167. 前記データ処理装置は、前記第2のモジュールに格納された前記署名データを検証して、前記コンテンツファイルの作成者および配給者と、前記キーファイルの作成者および配給者との正当性のうち少なくとも一つを確認する

請求項166に記載のデータ提供システム。

168. 前記データ提供装置は、前記コンテンツデータが圧縮されている場合に、当該コンテンツデータを伸長する伸長用ソフトウェアを前記コンテンツファイルにさらに格納する

請求項162に記載のデータ提供システム。

169. 前記データ提供装置は、前記コンテンツデータの内容の説明に関するメタデータを前記コンテンツファイルに格納して、あるいは前記コンテンツファイルとは別に前記データ配給装置に配給する

請求項162に記載のデータ提供システム。

170. 前記データ提供装置は、前記コンテンツファイルに電子透かし情報が埋め込まれている場合に、当該電子透かし情報を検出するのに用いられる情報を含む電子透かし情報モジュールを前記コンテンツファイルにさらに格納する

請求項162に記載のデータ提供システム。

171. 前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、

前記配信用鍵データを前記データ処理装置に配給する

請求項 162 に記載のデータ提供システム。

172. 前記管理装置および前記データ処理装置は、有効期間が規定された複数の配信用鍵データを有し、対応する期間の前記配信用鍵データを用いる

請求項 171 に記載のデータ提供システム。

173. 前記管理装置は、前記権利書データの文法を記述したデータをさらに格納した前記キーファイルを作成する

請求項 162 に記載のデータ提供システム。

174. 前記管理装置は、前記コンテンツファイルおよび前記キーファイルを読み込むための情報を示すデータであるファイルリードを前記データ処理装置に配給し、

前記データ処理装置は、前記ファイルリードに基づいて、前記コンテンツファイルおよび前記キーファイルの読み込みを行う

請求項 162 に記載のデータ提供システム。

175. 前記データ提供装置は、前記コンテンツファイルおよび前記キーファイルを読み込むための情報を示すデータであるファイルリードをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記ファイルリードに基づいて、前記コンテンツファイルおよび前記キーファイルの読み込みを行う

請求項 162 に記載のデータ提供システム。

176. 前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する

請求項 165 に記載のデータ提供システム。

177. 前記データ提供装置は、前記公開鍵データの正当性を証明する公開鍵

証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 176 に記載のデータ提供システム。

178. 前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 176 に記載のデータ提供システム。

179. 前記データ配給装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する

請求項 166 に記載のデータ提供システム。

180. 前記データ配給装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 179 に記載のデータ提供システム。

181. 前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 179 に記載のデータ提供システム。

182. 前記データ配給装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化した前記第2のモジュールを前記データ処理装置に送信する

請求項162に記載のデータ提供システム。

183. 前記データ配給装置は、前記モジュールを記録した記録媒体を作成する

請求項182に記載のデータ提供システム。

184. 前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項162に記載のデータ提供システム。

185. 前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する

請求項162に記載のデータ提供システム。

186. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項162に記載のデータ提供システム。

187. 前記管理装置は、コンテンツデータ単位で、前記利益分配処理を行う

請求項186に記載のデータ提供システム。

188. 前記データ配給装置は、前記コンテンツデータの価格を示す価格デー

タを格納した前記第2のモジュールを前記データ処理装置に配給する

請求項162に記載のデータ提供システム。

189. 前記管理装置は、前記データ配給装置から受けた前記価格データを登録する

請求項186に記載のデータ提供システム。

190. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを有する

請求項162に記載のデータ提供システム。

191. 前記第1のモジュールおよび前記第2のモジュールに、複数のコンテンツファイルと、当該複数のコンテンツファイルに対応する複数のキーファイルとが格納されている場合に、

前記第1のモジュールおよび前記第2のモジュールには、それぞれ前記複数のコンテンツファイルと、それらに対応するキーファイルとの対応関係を示すデータがさらに含まれている

請求項162に記載のデータ提供システム。

192. 前記データ提供装置は、複数の前記コンテンツファイルと、当該複数のコンテンツファイルにそれぞれ対応する複数のキーファイルとを格納したモジュールを前記データ処理装置に配給し、

前記コンテンツファイルには、前記複数のコンテンツファイル相互間の関係と、前記キーファイルとの関係とを示すディレクトリ構造データが含まれている

請求項162に記載のデータ提供システム。

193. 前記データ提供装置は、前記モジュールを格納する記憶回路をさらに有する

請求項162に記載のデータ提供システム。

194. 前記データ提供装置は、前記コンテンツデータに固有に割り付けられたコンテンツ識別子に基づいて、前記モジュールを管理する

請求項193に記載のデータ提供システム。

195. 前記管理装置は、前記コンテンツ識別子をさらに格納した前記キーファイルを作成する

請求項194に記載のデータ提供システム。

196. 前記コンテンツ識別子は、前記データ提供装置が前記記憶回路に格納するコンテンツデータ内でユニークに決められている

請求項194に記載のデータ提供システム。

197. 前記コンテンツ識別子は、前記グローバルユニークに決められている

請求項194に記載のデータ提供システム。

198. 前記データ提供装置は、前記コンテンツ識別子を生成する

請求項194に記載のデータ提供システム。

199. 前記データ提供装置は、前記モジュールを格納する記憶回路

をさらに有する請求項194に記載のデータ提供システム。

200. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

201. データ提供装置から第1のデータ配給装置および第2のデータ配給装置にコンテンツデータを提供し、前記第1のデータ配給装置および前記第2のデータ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記第1のデータ配給装置、前記第2のデータ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記第1のデータ配給装置および前記第2のデータ配給装置に提供し、

前記第1のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、

前記第2のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第3のモジュールを前記データ処理装置に配

給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

202. 前記第1のデータ配給装置は、前記コンテンツデータの価格を示す第1の価格データを格納した前記第2のモジュールを前記データ処理装置に配給し

、
前記第2のデータ配給装置は、前記コンテンツデータの価格を示す第2の価格データを格納した前記第3のモジュールを前記データ処理装置に配給し

、
請求項201に記載のデータ提供システム。

203. 第1のデータ提供装置からデータ配給装置に第1のコンテンツデータを提供し、第2のデータ提供装置からデータ配給装置に第2のコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記第1のデータ提供装置、前記第2のデータ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化された第1のコンテンツ鍵データと前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のキーファイルと、暗号化された第2のコンテンツ鍵データと前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のキーファイルとを作成し、

前記第1のデータ提供装置は、前記第1のコンテンツ鍵データを用いて暗号化された前記第1のコンテンツデータを格納した第1のコンテンツファイ

ルと、前記管理装置から受けた前記第 1 のキーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記第 2 のデータ提供装置は、前記第 2 のコンテンツ鍵データを用いて暗号化された前記第 2 のコンテンツデータを格納した第 2 のコンテンツファイルと、前記管理装置から受けた前記第 2 のキーファイルとを格納した第 2 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第 1 のコンテンツファイル、前記第 1 のキーファイル、前記第 2 のコンテンツファイルおよび前記第 2 のキーファイルを格納した第 3 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 3 のモジュールに格納された前記第 1 のコンテンツ鍵データ、前記第 2 のコンテンツ鍵データ、前記第 1 の権利書データおよび前記第 2 の権利書データを復号し、当該復号した第 1 の権利書データに基づいて前記第 1 のコンテンツデータの取り扱いを決定し、前記復号した第 2 の権利書データに基づいて前記第 2 のコンテンツデータの取り扱いを決定する

データ提供システム。

204. 前記データ配給装置は、前記第 1 のコンテンツデータの価格を示す第 1 の価格データと、前記第 2 のコンテンツデータの価格を示す第 2 の価格データとをさらに格納した前記第 3 のモジュールを前記データ処理装置に配給する

請求項 203 に記載のデータ提供システム。

205. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを

作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

206. 前記コンテンツファイルおよび前記キーファイルには、相互間の対応関係を明示するためのデータが含まれる

請求項205に記載のデータ提供システム。

207. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルを、所

定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

208. 前記コンテンツファイルおよび前記キーファイルには、相互間の対応関係を明示するためのデータが含まれる

請求項207に記載のデータ提供システム。

209. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号し

た権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

210. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

211. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを

作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

2 1 2. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

2 1 3. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

2 1 4. データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵

データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

215. 前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する

請求項214に記載のデータ提供システム。

216. 前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用

いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 2 1 4 に記載のデータ提供システム。

2 1 7. 前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 2 1 4 に記載のデータ提供システム。

2 1 8. データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

219. データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

220. 前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する

請求項219に記載のデータ提供システム。

221. 前記管理装置は、前記コンテンツファイルを記憶および管理するデー

データベース、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 2 1 9 に記載のデータ提供システム。

2 2 2. 前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 2 1 9 に記載のデータ提供システム。

2 2 3. データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権

利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

224. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

225. 前記データベース装置は、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記格納しているコンテンツファイルおよびキーファイルを一元的に管理する

請求項224に記載のデータ提供システム。

226. 前記管理装置は、前記キーファイルを記憶および管理するデータベ-

ス、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 2 2 4 に記載のデータ提供システム。

2 2 7. 前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 2 2 4 に記載のデータ提供システム。

2 2 8. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコン

コンテンツデータの取り扱いを決定する

データ提供システム。

229. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

230. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツ

データについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルに対応する前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

231. 前記データベース装置は、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記格納しているコンテンツファイルおよびキーファイルを一元的に管理する

請求項230に記載のデータ提供システム。

232. 前記管理装置は、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

対応するデータ提供装置において、当該データ提供装置が提供する前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項230に記載のデータ提供システム。

233. 前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 2 3 0 に記載のデータ提供システム。

2 3 4. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

2 3 5. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

236. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロ

トコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

237. 前記データベース装置は、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記格納しているコンテンツファイルおよびキーファイルを一元的に管理する

請求項236に記載のデータ提供システム。

238. 前記管理装置は、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

対応するデータ提供装置において、当該データ提供装置が提供する前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項236に記載のデータ提供システム。

239. 前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項236に記載のデータ提供システム。

240. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記デー

データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルに対応する前記データ配給装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

241. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスタソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツ

データについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

242. データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納され

た前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る

データ提供システム。

243. 前記データ処理装置は、前記データ配給装置が行うコンテンツデータの配信サービスに関してのデータ配給装置用履歴データを前記データ配給装置に送り、

前記データ配給装置は、前記データ配給装置用履歴データに基づいて、課金処理を行う

請求項242に記載のデータ提供システム。

244. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータを提供し、

前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する

データ提供システム。

245. データ提供装置からデータ処理装置にコンテンツデータを配給するデ

ータ提供方法において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

246. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

247. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

248. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、

所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

249. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

250. データ提供装置からデータ処理装置にコンテンツデータを配給し、管

理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

251. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを

決定する

データ提供方法。

252. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

253. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して

個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

254. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

255. データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

256. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを、前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記デ

ータ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

257. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

258. データ提供装置からデータ配給装置にコンテンツデータを提供し、前

記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ配給装置に配給し、

前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

259. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

通データベース 820 からコンテンツファイル CF を得ると共に、EMD サービスセンタ 302 からサービスプロバイダ 310 にキーファイル KF を送るようにしてもよい。このとき、サービスプロバイダ 310 が得たコンテンツファイル CF を作成したコンテンツプロバイダ 301 に対応する EMD サービスセンタ 302 からサービスプロバイダ 310 にキーファイル KF が送られる。

サービスプロバイダ 310 は、共通データベース 840 から得たコンテンツファイル CF と、EMD サービスセンタ 302 から得たキーファイル KF と、プライスタグデータ 312 とを格納してセキュアコンテナ 842 を作成する。

共通データベース 830 は、複数のコンテンツプロバイダ 301 が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツ ID を用いて、コンテンツファイル CF を一元的に管理する。

また、図 141 に示すように、EMD サービスセンタ 302 が作成したキーファイル KF を、ユーザホームネットワーク 303、303a の SAM 305₁、305₁₂ などに送るようにしてもよい。このときも、SAM 305₁、305₁₂ などに提供されたコンテンツファイル CF を作成したコンテンツプロバイダ 301 に対応する EMD サービスセンタ 302 から SAM 305₁、305₁₂ などにキーファイル KF が送られる。

また、サービスプロバイダ 310 は、コンテンツファイル CF をユーザホームネットワーク 303 に配給する。プライスタグデータ 312 は、サービスプロバイダ 310 がユーザホームネットワーク 303 に配給してもよいし、EMD サービスセンタ 302 がユーザホームネットワーク 303、303a に配給してもよい。

第 8 実施形態

図 142 は、本発明の第 8 実施形態の EMD システムを説明するための図である。

本実施形態の EMD システムでは、例えば、コンテンツプロバイダ 301 から

EMDサービスセンタ 302 に提供されたマスタソースを用いて EMD サービスセンタ 302 が作成した図 5 (A) に示すコンテンツファイル CF、あるいはコンテンツプロバイダ 310 が作成して EMD サービスセンタ 302 に提供した図 5 (A) に示すコンテンツファイル CF と、EMD サービスセンタ 302 が作成した図 5 (B) に示すキーファイル KF とが、EMD サービスセンタ 302 によってサービスプロバイダ 310 を介して、あるいは直接的にユーザホームネットワーク 303 の SAM 305₁ に配信される。

ここで、サービスプロバイダ 310 は、コンテンツファイル CF の販売価格を示すプライスタグデータ 312 をユーザホームネットワーク 303 に送ると共に、プライスタグデータ 312 を EMD サービスセンタ 302 に登録して権威化する。

また、サービスプロバイダ 310 は、自らを、配信事業者として EMD サービスセンタ 302 に登録する。

本実施形態の EMD システムでは、ユーザホームネットワーク 303 の例えば SAM 305₁ が、サービスプロバイダ 310 あるいは EMD サービスセンタ 302 から得たコンテンツファイル CF およびキーファイル KF を、ユーザホームネットワーク 303 内の SAM 305₂ および/またはユーザホームネットワーク 303 a 内の SAM 305₁₂ などに配信する配信事業者となる。

但し、この場合に、例えば、EMD サービスセンタ 302 は、SAM 305₁ がコンテンツファイル CF に格納されたコンテンツデータ C を購入した後に、当該購入したコンテンツデータ C を、何らかの販売マージンを加えて販売（再配付）して利益を上げることが禁止する。

本実施形態の EMD システムでは、購入形態が未決定のコンテンツデータ C、あるいは、購入形態として再生課金が決定されているコンテンツデータ C を、販売利益マージンをとらずに再配付することを条件に、SAM 305₁ がコンテンツデータ C を他の SAM に複製することを許可する。なお、これを機器間再配布

と呼ぶ。

また、本実施形態のEMDシステムでは、SAM305₁がサービスプロバイダ310から配給を受けたコンテンツファイルCF（あるいはセキュアコンテナ）に関しては、販売利益マージンをとらない形態での機器間売買は許可される。

また、本実施形態では、SAM305₁が、販売利益マージンをとる形態でのコンテンツデータCの販売（配信）を行う場合には、SAM305₁はEMDサービスセンタ302に自らを配信事業者として登録して許諾を受けると共に、コンテンツデータCの販売価格を示すプライスタグデータ312をEMDサービスセンタ302に登録する。そして、SAM305₁は、サービスプロバイダ310を介さずに、EMDサービスセンタ302内のCFデータベース802aおよびKFデータベース153aから直接的にコンテンツファイルCFおよびキーファイルKFの配給を受ける。

第9実施形態

図143は、本発明の第9実施形態のEMDシステムを説明するための図である。

本実施形態のEMDシステムでは、コンテンツプロバイダ301のそれぞれが、コンテンツプロバイダとしての役割に加えて、EMDサービスセンタ302としての役割を果たすことを特徴としている。

おの場合に、複数のコンテンツプロバイダ301がある場合に、それぞれのコンテンツプロバイダ301は、それぞれのEMDサービスセンタ302としての役割を持つ。

コンテンツプロバイダ301は、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナ851をサービスプロバイダ310に配信する。

サービスプロバイダ310は、セキュアコンテナ851が格納したコンテン

ファイルCF、キーファイルKFに、さらにプライスタグデータ312を加えてセキュアコンテナ852を作成し、これをユーザホームネットワーク303に配信する。

ユーザホームネットワーク303、303aでは、キーファイルKF内に格納された権利書データ106に基づいてコンテンツファイルCFの購入形態などを決定し、それに応じた利用履歴データ308を作成し、これをコンテンツプロバイダ301内のEMDサービスセンタ302に送信する。

このとき、利用履歴データ308は、コンテンツプロバイダ301毎に作成される。

コンテンツプロバイダ301のEMDサービスセンタ302は、利用履歴データ308に基づいて、SAM305₁、305₁₂のユーザが支払った利益を、自らと対応するサービスプロバイダ310との間で分配する。

また、ユーザホームネットワーク303のCAモジュール311から、配信サービスに関する履歴データが対応するサービスプロバイダ310に送られ、サービスプロバイダ310において配信サービスに対しての課金処理が行われる。

本発明は上述した実施形態には限定されない。

上述した実施形態では、コンテンツデータとしてオーディオデータを用いる場合を例示したが、コンテンツデータとして、ビデオデータ、オーディオ・ビデオデータ、テキストデータおよびコンピュータプログラムなどを用いてもよい。

また、上述した実施形態では、EMDサービスセンタ102、302において、キーファイルKFを作成する場合を例示したが、コンテンツプロバイダ101、301においてキーファイルKFを作成することも可能である。

この場合に、図7に対応するキーファイルKFのフォーマットは、図144に示すようになる。図144に示すように、当該キーファイルKFは、コンテンツプロバイダ101、301の秘密鍵データK_{cp.s}を用いて作成された署名データが用いられる点を除いて、図7に示すキーファイルKFと基本的に同じ情報を有

している。

また、上述した実施形態では、ユーザホームネットワーク103, 303からEMDサービスセンタ102, 302に、利用制御状態データ166をリアルタイムで送信する場合を例示したが、利用制御状態データ166をコンテンツプロバイダ101, 301および／またはサービスプロバイダ310に送信するようにしてもよい。これにより、コンテンツプロバイダ101, 301およびサービスプロバイダ310は、自らが提供および配給したコンテンツの購入状況を即座に把握でき、その後のサービスに反映できる。

以下、上述した本実施形態のEMDシステムによる効果を、従来技術およびその問題点を述べながら再び説明する。

デジタル放送（データ放送）、インターネットなどのデジタルネットワークが発達していない時代に、デジタルコンテンツ（コンテンツデータ）を流用させる手段として使用されていたROM型記録媒体では、デジタルコンテンツを非暗号化の状態で記録して流用させていた。デジタルネットワークが発達していない時代では、これらのコンテンツの著作権保護をおこなうのは、ユーザホームネットワーク上でのユーザによるカジュアルコピーを防ぐ方法を考えるだけで良かった。

しかしながら、デジタルネットワークが発達してきた昨今では、非暗号化コンテンツが搭載されているROM型記録媒体を一般市民が、いつ、どこでも、自由に入手することができるために、各自がこれらを購入し、圧縮してネットワークにアップロードすることが簡単にできてしまう。特にインターネットは世界中につながっているネットワークなので、非暗号化コンテンツを無料でインターネット上にアップロードし、市民はそれを無料で自分の個人端末にダウンロードすることが可能となってしまう、コンテンツの権利者（コンテンツプロバイダ）の著作権を著しく侵害する可能性が出てきている。

また、非暗号化の状態でアップロードせず、自らが、そのコンテンツに対し、

独自方式の電子透かし情報を埋め込み、暗号化をおこなうことで独自方式の課金機能を備え、インターネット上で著作権の許可なしに、目の届かないところで勝手に、デジタルコンテンツの販売をおこなうことも可能となっている。このときは、売り上げの一部がコンテンツの権利者に還元されないで、コンテンツの権利者（コンテンツプロバイダ）の著作権を著しく侵害することになる。

また、著作権者の許諾を得て、売り上げの一部をコンテンツの権利者（コンテンツプロバイダ）に還元する契約を権利者側と事前におこなうことで、これらのデジタルコンテンツを配信して利益が得られる配信サービスをおこなうことが可能になるが、基本的にコンテンツプロバイダは、こういったコンテンツの２次利用による流通体系をあまり好ましく思っていない。コンテンツの２次利用によるビジネスとは、たとえばレンタルビジネス、中古販売などが相当する。

２次利用による配信サービスが登場する時は、必ず著作権侵害の問題が起こり、サービス自体を軌道に載せるまで時間がかかる。コンテンツプロバイダと事前契約をおこなうことなしに、まず配信サービスを始めてしまい、著作権侵害ということで問題になってから、権利者側への利益分配なり著作権保護が考慮され配信サービスとしての許諾が得られる。レンタルＣＤ、レンタルビデオが相当する。ゲームソフトの中古販売などは深刻な問題である。現在ゲームソフトの中古販売ビジネスでは、売り上げの利益の一部がコンテンツの権利者側に還元されないで、権利者側は裁判で告訴しているが却下され、権利者側にとって非常に酷になっている。新作ソフトの半額以下で大量に販売されるので、ユーザからしても魅力がある市場で、新作ソフトの売り上げにも影響を及ぼす。

コンテンツの２次利用というのは、本来コンテンツの権利者がＲＯＭ型記録媒体を流通手段とし、そのデジタルコンテンツ記録済のＲＯＭ型記録媒体を商品として流通させて利益を得ている訳で、それらを購入したユーザによって、その商品をさらに流通させることで、購入したユーザが利益を得ることは、たとえ利益の一部が還元されたとしても、（コンテンツプロバイダ）権利者側の立場からす

るとあまり好ましく思わない。映画コンテンツなどは、録音権／領布権というもののがコンテンツの権利者側に法律で保障されており、権利者が世に流通させたコンテンツを、それを購入した時点で、その購入ユーザの手元からは流通しないことを前提としている。ゲームソフトの権利者団体は、この領布権の権利をゲームソフトにも利用し、2次利用ビジネスの抑制を裁判で訴えている。

コンテンツの権利者は、自分が著作権を持っているデジタルコンテンツについては、それを流用させる流通業者を管理下においておきたい（誰に流通させているか、を知っておきたい）。自分が著作権を持っているデジタルコンテンツを流通させて配信サービスをおこない利益を得ることを希望している配信事業者がいる場合は、コンテンツの権利者から直接デジタルコンテンツを渡せるようなシステムが望ましい。

なお、ここで述べている流通業者とは、デジタルコンテンツの対価に、さらに何％かの利益マージンを徴収することで利益を得る業者を指す。

デジタルコンテンツを他機器／記録媒体へ渡すときに利益マージンを徴収する場合、そのコンテンツ売買セッション配信サービスとして定義し、利益マージンを徴収しない場合を機器間再配付として定義し、これは超流通の原理により合法である。

コンテンツプロバイダが流通させた非暗号化コンテンツが記録されているROM型記録媒体からサービスプロバイダが、自分の配信サービス用コンテンツをオーサリングし、配信サービスをおこなう現状のデジタルコンテンツのネットワーク流通管理システムにおいて、コンテンツプロバイダが所有している一つのデジタルコンテンツが複数のサービスプロバイダによって配信される状況を考えると、同一コンテンツであるにも関わらず、各々のサービスプロバイダが採用するCAMモジュール／電子決済ツールにて権利処理がおこなわれるようにオーサリングされるため、使用される暗号鍵（コンテンツ鍵データ）、コンテンツの使用許諾条件（権利書データ）のフォーマットが各サービスプロバイダによって各々異な

り、ユーザホームネットワーク上で共通の権利処理ルールを提供することができない。こういった場合は、CAモジュール／電子決済ツールで利用する鍵データ類をすべてネットワーク機器のCAモジュール／電子決済ツールで清算し、あとはSCMSのルールに準拠することでユーザホームネットワーク上での共通の権利処理ルールを実現している。

また、CAモジュール／電子決済ツールの鍵で暗号化されたコンテンツと鍵データを、そのままネットワーク機器を通過してユーザホームネットワークバス（IEEE1394など。）を経由してストレージ機器の記録媒体に記録し、1394バス上につながる機器から遠隔的にネットワーク機器を経由してコンテンツの購入、決済処理ができたとしても、暗号化コンテンツを復号するためのデスクランブラがネットワーク機器に存在するので、結局再生時にネットワーク機器まで、コンテンツと鍵データを戻さないと再生できない（ネットワークCA）。

上述したように、現在までに世の中に広く流通している非暗号化コンテンツが記録されているROM型記録媒体の存在が、現状のデジタルコンテンツネットワーク配信サービスにとって問題の根源となっている。デジタルコンテンツのコンテンツ形態が、コンテンツプロバイダ以外の第三者によって作成される可能性を持っており、さらに、ユーザに対して、そのコンテンツを販売した人が、その対価を入手するシステムであるため、コンテンツの2次利用などコンテンツプロバイダの利益が不当に損なわれる可能性がある。また、オーサリングしたデジタルコンテンツの流通管理をコンテンツプロバイダが厳密におこなっていないため、自分が著作権を持っているデジタルコンテンツが稼ぎ出す全利益、およびそこから自分の利益分が還元されているかどうかを監視することが難しい。

前述した本実施形態のEMDシステムは、上述したような従来の問題を解決した。

すなわち、本実施形態のEMDシステムでは、コンテンツプロバイダがオーサリングしたデジタルコンテンツは、すべてコンテンツプロバイダ側で、コンテン

ツ形態や権利書データを作成し、コンテンツプロバイダ側のデータベースに管理しておく。コンテンツの権利書データに関しては、さらに第3の信頼機関であるEMDサービスセンタ（クリアリングハウス）で権威化し登録しておく。

こうすることで、コンテンツプロバイダの関係者が、デジタルコンテンツの権利処理ルールを完全に自分の管理下におくことができ、流通経路をコンテンツプロバイダ側で管理することを可能とする。また本件では、このコンテンツプロバイダ側で作成した権利書のデータの内容を、ユーザとの間に存在する流通業者が見ることができないような仕掛けを提供する。

また、本実施形態のEMDシステムでは、ROM型記録媒体を、ひとつの流通手段として考えて、そこに搭載するデジタルコンテンツの存在をROM型記録媒体から遊離させる。流通手段、流通経路によらず、デジタルコンテンツ単体で、その存在価値を表現するコンテンツ形態を提案する。デジタルコンテンツはコンテンツプロバイダ側である規定の形式で管理されるので、ROM型記録媒体に、その形式のデジタルコンテンツを搭載すると考えることで、ROM型記録媒体で流通されようが、デジタルネットワークで流通されようが、ユーザホームネットワーク上では、ROM→RAM、ネットワーク→RAMにおいて共通の権利処理ルールを提供することが可能となる。デジタルコンテンツの販売セッションを、すべてコンテンツプロバイダが規定、管理する形式でおこなう。これにより、流通手段、流通経路によらない共通の権利処理が可能となる。また、このコンテンツプロバイダ側で規定されたコンテンツ形態は、デジタルコンテンツの売買をおこなう上での最小単位と定義することで、その後の流通過程で利用されるコンテンツ形態の種類に依存せず共通の権利処理ルールを提供することができる。ユーザホームネットワークで購入したときに生成される課金情報を、サービスプロバイダに返すのではなく、第3の信頼機関であるEMDサービスセンタに返し、そこからサービスプロバイダに返すことによりコンテンツの2次利用によるビジネスの問題点を解決した。

以上説明したように、本発明によれば、データ提供装置が提供したコンテンツデータのデータ処理装置における取り扱いを、データ提供装置による権利書データに基づいて行わせることが可能になる。

その結果、データ提供装置の関係者によるコンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。

請求の範囲

1. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

2. 前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを前記キーファイルに付加する

請求項1に記載のデータ提供システム。

3. 前記データ提供装置は、前記コンテンツデータを格納したコンテンツファイルを作成し、当該コンテンツファイルを前記データ処理装置に提供する

請求項1に記載のデータ提供システム。

4. 前記データ提供装置は、前記コンテンツファイルの作成者の正当性を検証するための署名データを前記コンテンツファイルに付加する

請求項3に記載のデータ提供システム。

5. 前記データ提供装置は、前記権利書データを作成して前記管理装置に送り、

前記データ処理装置は、前記権利書データに基づいて、前記配給を受

けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項 1 に記載のデータ提供システム。

6. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

7. 前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する

請求項 6 に記載のデータ提供システム。

8. 前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する

請求項 6 に記載のデータ提供システム。

9. 前記データ提供装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記モジュールを前記データ処理装置に配給する

請求項 7 に記載のデータ提供システム。

10. 前記データ処理装置は、前記モジュールに格納された前記署名データを検証して、前記コンテンツファイルの作成者および配給者と、前記キーファイルの作成者および配給者との正当性のうち少なくとも一つを確認する

請求項 9 に記載のデータ提供システム。

11. 前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、

前記配信用鍵データを前記データ処理装置に配給する

請求項 6 に記載のデータ提供システム。

12. 前記管理装置および前記データ処理装置は、有効期間が規定された複数の配信用鍵データを有し、対応する期間の前記配信用鍵データを用いる

請求項 11 に記載のデータ提供システム。

13. 前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する

請求項 10 に記載のデータ提供システム。

14. データ提供装置からデータ処理装置にコンテンツデータを配給し、管

理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

15. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

データ提供システム。

16. データ提供装置からデータ処理装置にコンテンツデータを配給し、管

理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

17. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

18. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

19. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

20. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

21. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

22. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

23. 前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

請求項22に記載のデータ提供システム。

24. 前記データ配給装置は、前記提供を受けた第1のモジュールを包括さ

せた前記第2のモジュールを作成し、当該作成した第2のモジュールを前記データ処理装置に配給する

請求項22に記載のデータ提供システム。

25. 前記データ配給装置は、前記コンテンツデータの価格を示す価格データをさらに格納した前記第2のモジュールを前記データ処理装置に配給する

請求項22に記載のデータ提供システム。

26. 前記データ配給装置は、前記データ提供装置が前記コンテンツデータについて決定した卸売価格に基づいて、前記価格データを決定する

請求項25に記載のデータ提供システム。

27. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第1のモジュールを前記データ配給装置に提供する 請求項22に記載のデータ提供システム。

28. 前記データ配給装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第2のモジュールを前記データ処理装置に提供する 請求項22に記載のデータ提供システム。

29. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項 2 2 に記載のデータ提供システム。

3 0. 前記データ処理装置は、前記データ配給装置の前記配給に関しての配給履歴データを前記データ配給装置に送信し、

前記データ配給装置は、前記配給履歴データに基づいて、前記配給に関しての課金処理を行う

請求項 2 2 に記載のデータ提供システム。

3 1. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

3 2. 前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書デ

ータを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、前記受信した前記コンテンツ鍵データおよび前記権利書データを登録する

請求項 3 1 に記載のデータ提供システム。

3 3. 前記データ提供装置は、前記コンテンツファイルの作成者および提供者と、前記キーファイルの提供者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第 1 のモジュールを前記データ処理装置に配給する

請求項 3 1 に記載のデータ提供システム。

3 4. 前記データ配給装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第 2 のモジュールを前記データ処理装置に配給する

請求項 3 1 に記載のデータ提供システム。

3 5. 前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する

請求項 3 3 に記載のデータ提供システム。

3 6. 前記データ提供装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 3 3 に記載のデータ提供システム。

37. 前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項36に記載のデータ提供システム。

38. 前記データ配給装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する

請求項33に記載のデータ提供システム。

39. 前記データ配給装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項38に記載のデータ提供システム。

40. 前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項38に記載のデータ提供システム。

41. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処

理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項 31 に記載のデータ提供システム。

42. 前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第2のモジュールを前記データ処理装置に配給する。

請求項 31 に記載のデータ提供システム。

43. 前記管理装置は、前記データ配給装置から受けた前記価格データを登録する

請求項 42 に記載のデータ提供システム。

44. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを有する

請求項 31 に記載のデータ提供システム。

45. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

46. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

47. 前記コンテンツファイルおよび前記キーファイルには、相互の対応関係を明示するためのデータが含まれる

請求項 46 に記載のデータ提供システム。

48. データ提供装置からデータ処理装置にコンテンツデータを配給し、管

理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

49. 前記コンテンツファイルおよび前記キーファイルには、相互の対応関係を明示するためのデータが含まれる

請求項48に記載のデータ提供システム。

50. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化され

たコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第 2 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

51. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

52. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

53. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

5 4. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

5 5. データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

56. 前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する

請求項55に記載のデータ提供システム。

57. 前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用

いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 5 に記載のデータ提供システム。

58. データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

59. データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前

記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

60. 前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する

請求項59に記載のデータ提供システム。

61. データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを

前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

62. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

63. データ提供装置、データ配給装置、管理装置、データベース装置および

びデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

64. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテン

ツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

6 5. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

6 6. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデー

タを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

67. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテン

ツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

68. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

69. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベ

ース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

70. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデー

タを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

71. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

72. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ

提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

73. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

74. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

75. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格

納したコンテンツファイルを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

データ提供方法。

7.6. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

データ提供方法。

7.7. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供方法。

78. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

79. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

80. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

81. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを前記データ提供装置から前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供方法。

82. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを、前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該

復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

8 3. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第 2 のモジュールを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

8 4. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファ

イルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ配給装置に配給し、

前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

85. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルを前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

86. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

87. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管

理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供方法。

88. データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号

した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

89. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供方法。

90. データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コン

テンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

9 1. データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコン

テンツデータの取り扱いを決定する

データ提供方法。

9 2. データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

9 3. データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コン

テンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

94. データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

95. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

96. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

97. データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

98. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

99. 複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテン

を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310
に関しての処理を行う点を除いて、図26～図41などを用いて前述した第1実施
形態のSAM105、と基本的に行なう機能および構造を有している。

また、SAM305_a～305_dは、SAM305、と基本的に同じ機能を有
している。

すなわち、SAM305_a～305_dは、コンテンツ単位の課金処理をおこな
うモジュールであり、EMDサービスセンタ302との間で通信を行う。

以下、SAM305_aの機能について詳細に説明する。

図76は、SAM305_aの機能の構成図である。

なお、図76には、サービスプロバイダ310からセキュアコンテナ304を
入力する際の処理に関連するデータの流れが示されている。

図76に示すように、SAM305_aは、相互認証部170、暗号化・復号部
171、172、173、誤り訂正部181、ダウンロードメモリ管理部182
、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMD
サービスセンタ管理部185、利用監視部186、署名処理部189、SAM管
理部190、記憶部192、メディアSAM管理部197、スタックメモリ20
0、サービスプロバイダ管理部580、課金処理部587、署名処理部598お
よび外部メモリ管理部811を有する。

なお、図76に示すSAM305_aの所定の機能は、SAM105_aの場合と
同様に、CPUにおいて秘密プログラムを実行することによって実現される。

図76において、図26と同じ符号を付した機能ブロックは、第1実施形態で
説明した同一符号の機能ブロックと同じである。

また、図74に示す外部メモリ201には、第1実施形態で説明した処理およ
び後述する処理を経て、利用履歴データ308およびSAM登録リストが記憶さ
れる。

また、スタックメモリ200には、図77に示すように、コンテンツ鍵データ

K_c、権利書データ(UCP)106、記憶部192のロック鍵データK_{Loc}、コンテンツプロバイダ301の公開鍵証明書データCER_{cp}、サービスプロバイダ310の公開鍵証明書データCER_{sp}、利用制御状態データ(UCS)366、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃およびプライスタグデータ312などが記憶される。

以下、SAM305の機能ブロックのうち、図76において新たに符号を付した機能ブロックについて説明する。

署名処理部589は、記憶部192あるいはスタックメモリ200から読み出したEMDサービスセンタ302の公開鍵データK_{sec.p}、コンテンツプロバイダ301の公開鍵データK_{cp}、およびサービスプロバイダ310の公開鍵データK_{sp}を用いて、セキュアコンテナ304内の署名データの検証を行なう。

課金処理部587は、図78に示すように、図74に示す購入・利用形態決定操作部165からの操作信号S165と、スタックメモリ200から読み出されたプライスタグデータ312とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。

課金処理部587による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

また、課金処理部587は、課金処理において、利用履歴データ308を生成し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。

ここで、利用履歴データ308は、第1実施形態の利用履歴データ108と同様に、EMDサービスセンタ302において、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。

また、課金処理部587は、操作信号S165に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態(UCS: Usage Control Status)

データ166を生成し、これをスタックメモリ200に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ166には、コンテンツのID、購入形態、買い切り価格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

なお、決定された購入形態が再生課金である場合には、例えば、SAM305₁からサービスプロバイダ310に利用制御状態データ166をリアルタイムに送信し、サービスプロバイダ310がEMDサービスセンタ302に、利用履歴データ308をSAM105₁に取りに行くことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、サービスプロバイダ310およびEMDサービスセンタ302にリアルタイムに送信される。

また、SAM305₁では、図76に示すように、EMDサービスセンタ管理部185を介してEMDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図74に示す復号モジュール905から入力したセキュアコンテナ304のうち、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304が誤り訂正部181に出力される。これにより、SAM305₁において、当該SAM305₁のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコン

テンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる。

以下、SAM305₁内での処理の流れを説明する。

EMDサービスセンタ302から受信した配信用鍵データKD₁～KD₉を記憶部192に格納する際のSAM305₁内での処理の流れは、前述したSAM105₁の場合と同様である。

次に、セキュアコンテナ304をサービスプロバイダ310から入力する際のSAM305₁内での処理の流れを図76を参照しながら説明する。

相互認証部170と図63に示すサービスプロバイダ310の相互認証部352との間で相互認証が行なわれる。

暗号化・復号部171は、当該相互認証によって得られたセッション鍵データK_{ss}を用いて、サービスプロバイダ管理部580を介してサービスプロバイダ310から受信した図65に示すセキュアコンテナ304を復号する。

次に、署名処理部589は、図65(D)に示す署名データSIG_{s1,ssc}, SIG_{1,ssc}の検証を行った後に、公開鍵証明書データCER_{sp}, CER_{cp}内に格納された公開鍵データK_{sp,p}, K_{cp,p}を用いて、署名データSIG_{s,cp}, SIG_{s2,sp}, SIG_{7,cp}, SIG_{s2,sp}, SIG_{s4,sp}の正当性を検証する。

ここで、署名データSIG_{s,cp}, SIG_{s2,sp}を検証することでコンテンツファイルCFの作成者および送信者の正当性が確認され、署名データSIG_{7,cp}, SIG_{s3,sp}を検証することでキーファイルKFの送信者の正当性が確認され、署名データSIG_{s4,sp}を検証することでプライスタグデータ312の作成者および送信者の正当性が確認される。

また、署名処理部589は、記憶部192から読み出した公開鍵データK_{ssc}, pを用いて、図65(B)に示すキーファイルKFに格納された署名データSIG_{s1,ssc}の正当性を検証することで、キーファイルKFの作成者の正当性、並びにキーファイルKFがEMDサービスセンタ302で登録されているか否かを検

証する。

サービスプロバイダ管理部 580 は、署名処理部 589 において上述した全ての署名データの正当性が確認されると、セキュアコンテナ 304 を誤り訂正部 181 に出力する。

誤り訂正部 181 は、セキュアコンテナ 304 を誤り訂正した後に、ダウンロードメモリ管理部 182 に出力する。

ダウンロードメモリ管理部 182 は、相互認証部 170 と図 74 に示すメディア SAM167a との間で相互認証を行なった後に、セキュアコンテナ 304 をダウンロードメモリ 167 に書き込む。

次に、ダウンロードメモリ管理部 182 は、相互認証部 170 と図 74 に示すメディア SAM167a との間で相互認証を行なった後に、セキュアコンテナ 304 に格納された図 65 (B) に示すキーファイル KF をダウンロードメモリ 167 から読み出してセキュアコンテナ復号部 183 に出力する。

そして、セキュアコンテナ復号部 183 は、記憶部 192 から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_n$ を用いて、図 65 (B) に示すキーファイル KF に格納されたコンテンツ鍵データ Kc 、権利書データ 106 および SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_n$ が復号される。

そして、復号されたコンテンツ鍵データ Kc 、権利書データ 106 および SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_n$ がスタックメモリ 200 に書き込まれる。

以下、サービスプロバイダ 310 からダウンロードメモリ 167 にダウンロードされたセキュアコンテナ 304 の購入形態を決定するまでの処理の流れを図 78 および図 79 を参照しながら説明する。

図 79 は、セキュアコンテナ 304 の購入形態決定処理を説明するためのフローチャートである。

<ステップ E1>

ユーザによる図 7 4 に示す購入・利用形態決定操作部 1 6 5 の操作によって、試験モードを示す操作信号 S 1 6 5 が課金処理部 5 8 7 に出力された場合には、ステップ E 2 の処理が行われ、そうでない場合にはステップ E 3 の処理が行われる。

<ステップ E 2>

試験モードを示す操作信号 S 1 6 5 が課金処理部 5 8 7 に出力された場合に行われ、例えば、ダウンロードメモリ 1 6 7 に記憶されているコンテンツファイル CF が、復号・伸長モジュール管理部 1 8 4 を介して、図 7 4 に示す復号・伸長モジュール 1 6 3 に出力される。

このとき、コンテンツファイル CF に対して、相互認証部 1 7 0 とメディア SAM 1 6 7 a との間の相互認証およびセッション鍵データ K_{ses} による暗号化・復号と、相互認証部 1 7 0 と相互認証部 2 2 0 との間の相互認証およびセッション鍵データ K_{ses} による暗号化・復号とが行なわれる。

コンテンツファイル CF は、図 7 4 に示す復号部 2 2 1 においてセッション鍵データ K_{ses} を用いて復号された後に、復号部 2 2 2 に出力される。

また、スタックメモリ 2 0 0 から読み出されたコンテンツ鍵データ K c および半開示パラメータデータ 1 9 9 が、図 7 4 に示す復号・伸長モジュール 1 6 3 に出力される。このとき、相互認証部 1 7 0 と相互認証部 2 2 0 との間の相互認証後に、コンテンツ鍵データ K c および半開示パラメータデータ 1 9 9 に対してセッション鍵データ K_{ses} による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ 1 9 9 が半開示処理部 2 2 5 に出力され、半開示処理部 2 2 5 からの制御によって、復号部 2 2 2 によるコンテンツ鍵データ K c を用いたコンテンツデータ C の復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータ C が、伸長部 2 2 3 において伸長された後に、電子透かし情報処理部 2 2 4 に出力される。

次に、電子透かし情報処理部 2 2 4 においてユーザ電子透かし情報用データ 1

96がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。

<ステップE3>

ユーザが、購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

<ステップE4>

課金処理部187において、決定された購入形態に応じた利用履歴データ308および利用制御状態データ166が生成され、利用履歴データ308が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

そして、スタックメモリ200に格納されているキーファイルKFと、利用制御状態データ166とを用いて、購入形態が決定した後述する図81(C)に示す新たなキーファイルKF₁が生成され、当該作成されたキーファイルKF₁がスタックメモリ200に記憶される。

図81(C)に示すように、キーファイルKF₁に格納された利用制御状態データ166はストレージ鍵データK_{STR}およびメディア鍵データK_{MED}を用いてDESのCBCモードを利用して順に暗号化されている。

ここで、記録用鍵データK_{STR}は、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。また、メディア鍵データK_{MED}は、記

録媒体にユニークなデータである。

また、署名処理部589において、SAM305₁の秘密鍵データ $K_{SAM1.s}$ を用いて、キーファイル KF_1 のハッシュ値 H_{K1} が作成され、当該作成されたハッシュ値 H_{K1} が、キーファイル KF_1 と対応付けられて、スタックメモリ200に記憶される。

<ステップE5>

SAM305₁からEMDサービスセンタ302に、利用制御状態データ166が送信される。当該利用制御状態データ166の送信は、SAM305₁において、コンテンツデータの購入形態が決定される度に行われる。

なお、SAM305₁からEMDサービスセンタ302への利用履歴データ308の送信は、例えば、例えば、1箇月などの所定の時間間隔で行われる。

次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図78を参照しながら説明する。

この場合には、利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、図74に示す復号・伸長モジュール163に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcが復号・伸長モジュール163に出力される。

そして、復号・伸長モジュール163の復号部222において、コンテンツ鍵データKcを用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。

このとき、課金処理部587において、操作信号S165に応じて、外部メモリ201に記憶されている利用履歴データ308が更新される。

利用履歴データ308は、秘密鍵データ $K_{SAM1.s}$ を用いて作成した署名データ

SIG_{208, SAM1}と共に、EMDサービスセンタ管理部185を介して、所定のタイミングで、EMDサービスセンタ302に送信される。

次に、図80に示すように、例えば、ネットワーク機器360₁のダウンロードメモリ167にダウンロードされた既に入力形態が決定された図81に示すセキュアコンテナ304xを、バス191を介して、AV機器360₂のSAM305₂に転送する場合のSAM305₁内での処理の流れを図82を参照しながら説明する。

ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器360₂に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部587に出力される。

これにより、課金処理部587は、操作信号S165に基づいて、スタックメモリ200に記憶されている利用履歴データ308を更新する。

また、ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図81(A), (B), (C)に示すコンテンツファイルCFおよびキーファイルKF、KF₁を署名処理部589およびSAM管理部190に出力する。

そして、署名処理部589は、コンテンツファイルCFおよびキーファイルKFの署名データSIG_{41, SAM1}, SIG_{42, SAM1}を作成すると共に、キーファイルKF₁のハッシュ値H_{K1}を作成し、これらをSAM管理部190に出力する。

また、SAM管理部190は、図81(D), (E)に示すプライスタグデータ312およびその署名データSIG_{44, SP}と、公開鍵証明書データCER_{CP}およびその署名データSIG_{1, SSC}とをスタックメモリ200から読み出す。

また、SAM管理部190は、図81(E)に示す公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22, SSC}を記憶部192から読み出す。

次に、SAM管理部190は、図81に示すセキュアコンテナ304xを作成

する。

また、相互認証部170は、SAM305₂との間で相互認証を行って得たセッション鍵データK_{ss}を暗号化・復号部171に出力する。

SAM管理部190は、図81に示すセキュアコンテナ304xを、暗号化・復号部171において、セッション鍵データK_{ss}を用いて暗号化した後に、図82に示すAV機器360₂のSAM305₂に出力する。

以下、図80に示すように、SAM305₁から入力したセキュアコンテナ304xを、RAM型などの記録媒体（メディア）に書き込む際のSAM305₂内での処理の流れを、図83を参照しながら説明する。

この場合には、SAM305₂のSAM管理部190は、図83に示すように、図81に示すセキュアコンテナ304xを、ネットワーク機器360₁のSAM305₁から入力する。

そして、SAM305₁の相互認証部170とSAM305₂の相互認証部170との間の相互認証が行われ、署名処理部589において、当該相互認証によって得られたセッション鍵データK_{ss}を用いて、セキュアコンテナ304xの復号が行われる。

次に、署名処理部589において、記憶部192から読み出した公開鍵データK_{esc, P}を用いて、図81(E)に示す署名データSIG_{61, ESC}, SIG_{1, ESC}, SIG_{22, ESC}の正当性を検証する。

そして、署名データSIG_{61, ESC}, SIG_{1, ESC}, SIG_{22, ESC}の正当性が確認されると、署名処理部589において、公開鍵証明書データCER_{SP}, CER_{CP}, CER_{SAM1}に含まれる公開鍵データK_{SP, P}, K_{CP, P}, K_{SAM1, P}を用いて、図81(A)～(D)に示す署名データSIG_{6, CP}, SIG_{62, SP}, SIG_{41, SAM1}, SIG_{7, CP}, SIG_{63, SP}, SIG_{42, SAM1}, SIG_{64, SP}およびハッシュ値H_{K1}の正当性が検証される。

そして、これらの署名データの正当性が確認されると、スタックメモリ200

に、キーファイルKF、KF₁ およびブライスタグデータ312が記憶される。

また、コンテンツファイルCFが、SAM管理部190から記録モジュール管理部855に出力される。

そして、図81(C)に示すキーファイルKF₁に格納されたコンテンツ鍵データK_Cおよび利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において、記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED} および購入者鍵データK_{PIN}を用いて順に暗号化された後に記録モジュール管理部855に出力される。

また、スタックメモリ200から読み出されたキーファイルKFが、記録モジュール管理部855に出力される。

そして、相互認証部170とRAM型の記録媒体130、のメディアSAM133との間の相互認証を行った後に、コンテンツファイルCFがRAM型の記録媒体130、のセキュアでないRAM領域134に記憶され、キーファイルKF、KF₁ およびブライスタグデータ312がセキュアRAM領域132に書き込まれる。

なお、キーファイルKF、KF₁ およびブライスタグデータ312を、RAM型の記録媒体130、のメディアSAM133に記憶するようにしてもよい。

なお、SAM305、内での処理のうち、コンテンツの購入形態が未決定のROM型の記録媒体の購入形態を決定する際のAV機器360、内での処理の流れ、AV機器360、において購入形態が未決定のROM型の記録媒体からセキュアコンテナ304を読み出してこれをAV機器360、に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にブライスタグデータ312を格納する点を除いて、第1実施形態のSAM105、の場合と同じである。

次に、図59に示すEMDシステム300の全体動作について説明する。

図84および図85は、EMDシステム300の全体動作のフローチャートである。

ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテンツ304を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、EMDサービスセンタ302へのコンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄の登録は既に終了しているものとする。

ステップS21: EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データK_{CP}、Pの公開鍵証明書CER_{CP}を、自らの署名データSIG₁、_{sec}と共にコンテンツプロバイダ301に送信する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データK_{SP}、Pの公開鍵証明書CER_{SP}を、自らの署名データSIG₁、_{sec}と共にサービスプロバイダ310に送信する。

また、EMDサービスセンタ302は、各々有効期限が1カ月の3カ月分の配信用鍵データKD₁～KD₃をユーザホームネットワーク303のSAM305₁～305₄に送信する。

ステップS22: コンテンツプロバイダ301は、相互認証を行った後に、図18に示す登録用モジュールMod₂を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データKcを登録して権威化する。

また、EMDサービスセンタ302は、登録用モジュールMod₂に応じた図5(B)に示す6カ月分のキーファイルKFを作成し、これをコンテンツプロバイダ301に送信する。

ステップS23: コンテンツプロバイダ301は、図5(A)、(B)に示す

コンテンツファイルCFおよびその署名データSIG_{6,cf}と、キーファイルKFおよびその署名データSIG_{7,cf}とを作成し、これらと図5(C)に示す公開鍵証明書データCER_{ss}およびその署名データSIG_{1,ss}とを格納したセキュアコンテナ104を、オンラインおよび/またはオフラインで、サービスプロバイダ310に提供する。

ステップS24: サービスプロバイダ310は、図5(C)に示す署名データSIG_{1,ss}を検証した後に、公開鍵証明書データCER_{cf}に格納された公開鍵データK_{cf,r}を用いて、図5(A), (B)に示す署名データSIG_{6,cf}およびSIG_{7,cf}を検証して、セキュアコンテナ104が正当なコンテンツプロバイダ301から送信されたものであるかを確認する。

ステップS25: サービスプロバイダ310は、プライスタグデータ312およびその署名データSIG_{4,sp}を作成し、これらを格納した格納した図65に示すセキュアコンテナ304を作成する。

ステップS26: サービスプロバイダ310は、図69に示すプライスタグ登録要求モジュールMod₁₀₂を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、プライスタグデータ312を登録して権威化する。

ステップS27: サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテナ304を、オンラインあるいはオフラインで、図74に示すネットワーク機器360₁の復号モジュール905に送信する。

ステップS28: CAモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

ステップS29: SAM305₁~305₄のいずれかにおいて、図65(D)に示す署名データSIG_{1,ss}を検証した後に、公開鍵証明書データCER_{sp}に格納された公開鍵データK_{sp,r}を用いて、図65(A), (B), (C)に示

す署名データ $SIG_{s, sp}$, $SIG_{s, sp}$, $SIG_{s, sp}$ を検証して、セキュアコンテナ 304 内の所定のデータが正当なサービスプロバイダ 310 において作成および送信されたか否かを確認する。

ステップ S30: SAM305₁ ~ 305₄ のいずれかにおいて、図 65 (D) に示す署名データ $SIG_{1, esc}$ を検証した後に、公開鍵証明書データ CER_{op} に格納された公開鍵データ $K_{op, p}$ を用いて、図 65 (A), (B), (C) に示す署名データ $SIG_{s, sp}$, $SIG_{7, sp}$ を検証して、セキュアコンテナ 304 内のコンテンツファイル CF が正当なコンテンツプロバイダ 301 において作成されたか否かと、キーファイル KF が正当なコンテンツプロバイダ 301 から送信されたか否かを確認する。

また、SAM305₁ ~ 305₄ のいずれかにおいて、公開鍵データ $K_{esc, p}$ を用いて、図 65 (B) に示すキーファイル KF 内の署名データ $SIG_{k1, esc}$ の正当性を検証することで、キーファイル KF が正当な EMD サービスセンタ 302 によって作成されたか否かを確認する。

ステップ S31: ユーザが図 74 の購入・利用形態決定操作部 165 を操作してコンテンツの購入・利用形態を決定する。

ステップ S32: ステップ S31 において生成された操作信号 S165 に基づいて、SAM305₁ ~ 305₄ において、セキュアコンテナ 304 の利用履歴 (Usage Log) データ 308 が生成される。

SAM305₁ ~ 305₄ から EMD サービスセンタ 302 に、利用履歴データ 308 およびその署名データ $SIG_{205, SAM1}$ が送信される。

また、購入形態が決定される度にリアルタイムに、SAM305₁ ~ 305₄ から EMD サービスセンタ 302 に利用制御状態データ 166 が送信される。

ステップ S33: EMD サービスセンタ 302 は、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の各々について、課金内容を決定 (計算) し、その結果に基づいて、決済請求権データ 1

52c, 152sを作成する。

ステップS34: EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c, 152sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

以上説明したように、EMDシステム300では、図5に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理をSAM305₁～305₄内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁～KD₄を用いて暗号化されており、配信鍵データKD₁～KD₄を保持しているSAM305₁～305₄内でのみ復号される。そして、SAM305₁～305₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300にれば、権利書データ106をサービスプロバイダ310が管理できないようである。

そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を介してユーザホームネットワーク303にコンテンツデータCが配給

された場合でも、ユーザホームネットワーク 303 における当該コンテンツデータ C についての権利処理を、コンテンツプロバイダ 301 が作成した共通の権利書データ 106 に基づいて行わせることができる。

また、EMD システム 300 では、セキュアコンテナ 104、304 内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ 310 および SAM 305₁ ~ 305₄ において、それらの作成者および送信者の正当性、並びにそれらが改竄されていないか否かなどを確認できる。その結果、コンテンツデータ C の不正利用を効果的に回避できる。

また、EMD システム 300 では、サービスプロバイダ 310 からユーザホームネットワーク 103 へのコンテンツデータ C の配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ 304 を用いて行うことで、双方の場合において、SAM 305₁ ~ 305₄ におけるコンテンツデータ C の権利処理を共通化できる。

また、EMD システム 300 では、ユーザホームネットワーク 303 内のネットワーク機器 360₁ および AV 機器 360₂ ~ 360₄ においてコンテンツデータ C を購入、利用、記録および転送する際に、常に権利書データ 106 に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

例えば、図 86 に示すように、コンテンツプロバイダ 301 が提供したコンテンツデータ C を、サービスプロバイダ 310 からユーザホームネットワーク 303 に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法（経路）で配信（配給）した場合でも、ユーザホームネットワーク 303、303a の SAM において、コンテンツプロバイダ 301 が作成した権利書データ 106 に基づいて、共通の権利処理ルールが採用される。

また、EMD システム 300 によれば、EMD サービスセンタ 302 が、認証

機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。

また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM305₁～305₅に供給される。従って、SAM305₁～305₅において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。

すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

以下、上述した第2実施形態のEMDシステム300で採用するセキュアコンテナなどの配送プロトコルの具体例について説明する。

図87に示すように、コンテンツプロバイダ301において作成されたセキュアコンテナ104は、インターネット（TCP/IP）あるいは専用線（ATM Cell）などのコンテンツプロバイダ用配送プロトコルを用いてサービスプロバイダ310に提供される。

また、サービスプロバイダ310は、セキュアコンテナ104を用いて作成したセキュアコンテナ304を、デジタル放送（MPEG-TS上のXML/SMIL）、インターネット（TCP/IP上のXML/SMIL）あるいはパッケージ流通（記録媒体）などのサービスプロバイダ用配送プロトコルを用いてユーザホームネットワーク303に配給する。

また、ユーザホームネットワーク303、303a内、あるいはユーザホーム

ネットワーク 303 と 303a との間において、SAM 相互間で、セキュアコンテンツが、家庭内 EC / 配信サービス (1394 シリアルバス・インターフェイス上の XML / SMIL) や記録媒体などを用いて転送される。

以下、図 87 において、符号 A ~ G を用いた経路におけるデータ転送に採用される配送プロトコルの一例を詳細に説明する。

図 88 は、図 87 に示すコンテンツプロバイダ 301 とサービスプロバイダ 310 との間 (符号 A) でセキュアコンテンツ 104 などを配送するときに採用される配送プロトコルを説明するための図である。

図 88 に示すように、コンテンツプロバイダ 301 からサービスプロバイダ 310 にセキュアコンテンツ 104 などが、IP / IP-SEC 層、SSL (Secure Sockets Layer) 層、XML (eXtensible Markup Language) / SMIL (Synchronized Multimedia Integration Language) 層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

図 89 は、図 87 に示す EMD サービスセンタ 302 とコンテンツプロバイダ 301 との間 (符号 B) でキーファイルなどを配送するときに採用される配送プロトコルを説明するための図である。

図 89 に示すように、EMD サービスセンタ 302 からコンテンツプロバイダ 301 にキーファイルなどが、IP / IP-SEC 層、SSL 層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

図 90 は、図 87 に示す EMD サービスセンタ 302 とサービスプロバイダ 310 との間 (符号 C) でブライスタグデータ 312 などを配送するときに採用される配送プロトコルを説明するための図である。

図 90 に示すように、EMD サービスセンタ 302 からサービスプロバイダ 310 にブライスタグデータ 312 などが、IP / IP-SEC 層、SSL 層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

図91は、図87に示すサービスプロバイダ310とユーザホームネットワーク303との間（符号D）、ユーザホームネットワーク303内（符号E）で、セキュアコンテナ304などを配送するときに採用される配送プロトコルを説明するための図である。

図91に示すように、サービスプロバイダ310からユーザホームネットワーク303のネットワーク機器360₁にセキュアコンテナ304などが配送される。

このとき、サービスプロバイダ310とネットワーク機器360₁の間では、MPEG-TS層、PES層またはDSM-CC_Data_Carousel層、および、MHEG(Multimedia and Hypermedia Experts)層または「http層およびXML/SMIL層」が、セキュアコンテナ304を転送するためのサービスプロバイダ用商品配送プロトコルとして用いられる。

また、ネットワーク機器360₁とストレージ機器360₂との間、並びにAV機器相互間では、HAVi(XML)が、セキュアコンテナを転送するためのユーザホームネットワーク商品配送プロトコルとして用いられる。

このとき、デジタル放送のデータ放送方式にXML/SMIL/BMLを利用した場合には、セキュアコンテナ304のコンテンツファイルCF1、CF2およびキーファイルKF1、KF2と視聴（デモ）サンプルは、図92に示すようにHTTP層上のBML/XML/SMIL層およびモノメディアデータ層に格納されて配送される。

また、デジタル放送のデータ放送方式にMHEGを利用した場合には、セキュアコンテナ304のコンテンツファイルCF1、CF2およびキーファイルKF1、KF2と視聴（デモ）サンプルは、図93に示すようにMHEG層上のモノメディアデータ層に格納されて配送される。

また、デジタル放送のデータ放送方式にXML/SMILを利用した場合には、セキュアコンテナ304のコンテンツファイルCF1、CF2およびキーファ

イルKF1, KF2と視聴(デモ)サンプルは、図94に示すようにHTTP層上のXML/SMIL層に格納されて配送される。

図95は、図87に示すEMDサービスセンタ302とユーザホームネットワーク303, 303aとの間(符号G)で、利用履歴データ308および利用制御状態データ166などを配送するときに採用される配送プロトコルを説明するための図である。

図95に示すように、ネットワーク機器360₁からEMDサービスセンタ302に、利用履歴データ308などが転送される場合に、IP/IP-SEC層、SSL層およびアプリケーション層において、セッション鍵データを用いたセッションが行われる。

また、ネットワーク機器360₂などがEMDサービスセンタ302に利用履歴データ308および利用制御状態データ166などを転送する場合には、利用履歴データ308などが、IP/IP-SEC層およびHAVI層でセッションを行ってストレージ機器360₂からネットワーク機器360₁に転送された後に、ネットワーク機器360₁からEMDサービスセンタ302に前述したように転送される。

図96は、図87に示すユーザホームネットワーク303のストレージ機器360₄からユーザホームネットワーク303aのストレージ機器360₁₁に、セキュアコンテナを配送するときに採用される配送プロトコルを説明するための図である。

図96に示すように、ストレージ機器360₄からストレージ機器360₁₁にセキュアコンテナが、IP/IP-SEC層、SSL層、XML/SMIL層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

。

第2実施形態の第1変形例

図97は、第2実施形態の第1変形例に係わる2個のサービスプロバイダを用

いたEMDシステム300aの構成図である。

図97において、図59と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。

図97に示すように、EMDシステム300aでは、コンテンツプロバイダ301からサービスプロバイダ310aおよび310bに、同じセキュアコンテナ104を供給する。

サービスプロバイダ310aは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312aとを格納したセキュアコンテナ304aを作成し、これをネットワーク機器360₁に配給する。

また、サービスプロバイダ310bは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312bとを格納したセキュアコンテナ304bを作成し、これをネットワーク機器360₁に配給する。

ここで、セキュアコンテナ304a、304bのフォーマットは、図65を用いた説明したセキュアコンテナ304と同じである。

ネットワーク機器360_{a1}には、サービスプロバイダ310a、310bの各々に対応したCAモジュール311a、311bが設けられている。

CAモジュール311a、311bは、自らの要求に応じたセキュアコンテナ304a、304bの配給を、それぞれサービスプロバイダ310a、310bから受ける。

次に、CAモジュール311a、311bは、配給されたセキュアコンテナ304a、304bに応じたSP用購入履歴データ309a、309bをそれぞれ作成し、これらをそれぞれサービスプロバイダ310a、310bに送信する。

また、CAモジュール311a, 311bは、セキュアコンテナ304a, 304bをセッション鍵データK_{ss}で復号した後に、SAM305₁～305₄に出力する。

次に、SAM305₁～305₄において、共通の配信用鍵データKD₁～KD₄を用いて、セキュアコンテナ304a, 304b内のキーファイルKFが復号され、共通の権利書データ106に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ308が作成される。

そして、SAM305₁～305₄からEMDサービスセンタ302に、利用履歴データ308が送信される。

EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310a, 310bの各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ152c, 152sa, 152sbを作成する。

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c, 152sa, 152sbを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310a, 310bの所有者に分配される。

上述したように、EMDシステム300aによれば、同じコンテンツファイルCFをサービスプロバイダに310a, 310bに供給する場合に、当該コンテンツファイルCFについての権利書データ106を配信用鍵データKD₁～KD₄で暗号化してサービスプロバイダに310a, 310bに供給し、サービスプロバイダに310a, 310bは暗号化された権利書データ106をそのまま格納したセキュアコンテナ304a, 304bをユーザホームネットワークに配給

する。そのため、ユーザホームネットワーク内のSAM305₁～305₄では、コンテンツファイルCFをサービスプロバイダに310_a、310_bの何れから配給を受けた場合でも、共通の権利書データ106に基づいて権利処理を行うことができる。

なお、上述した第1変形例では、2個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

第2実施形態の第2変形例

図98は、第2実施形態の第2変形例に係わる複数のコンテンツプロバイダを用いたEMDシステム300bの構成図である。

図98において、図59と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。

図98に示すように、EMDシステム300bでは、EMDサービスセンタ302からコンテンツプロバイダ301_a、301_bにそれぞれキーファイルKF_a、KF_bが供給され、コンテンツプロバイダ301_a、301_bからサービスプロバイダ310に、それぞれセキュアコンテナ104_a、104_bが供給される。

サービスプロバイダ310は、例えば、コンテンツプロバイダ301_a、301_bが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ104_aについてのプライスタグデータ312_aと、セキュアコンテナ104_bについてのプライスタグデータ312_bとをそれぞれ生成し、これらを格納したセキュアコンテナ304_cを作成する。

図98に示すように、セキュアコンテナ304_cには、コンテンツファイルCF_a、CF_b、キーファイルKF_a、KF_b、プライスタグデータ312_a、312_b、それらの各々についてのサービスプロバイダ310の秘密鍵データK_{cp}による署名データが格納されている。

セキュアコンテナ304_cは、ユーザホームネットワーク303のネットワー

ク機器 360₁ の CA モジュール 311 で受信された後に、SAM305₁ ~ 305₄ において処理される。

SAM305₁ ~ 305₄ では、配信用鍵データ KDa₁ ~ KDa₄ を用いて、キーファイル KFa が復号され、権利書データ 106a に基づいて、コンテンツファイル CFa についてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ 308 に記述される。

また、SAM305₁ ~ 305₄ において、配信用鍵データ KDb₁ ~ KDb₄ を用いて、キーファイル KFb が復号され、権利書データ 106b に基づいて、コンテンツファイル CFb についてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ 308 に記述される。

そして、SAM305₁ ~ 305₄ から EMD サービスセンタ 302 に、利用履歴データ 308 が送信される。

EMD サービスセンタ 302 では、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301a、301b およびサービスプロバイダ 310 の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ 152ca、152cb、152s を作成する。

EMD サービスセンタ 302 は、ペイメントゲートウェイ 90 を介して決済機関 91 に、決済請求権データ 152ca、152cb、152s を送信し、これにより、ユーザホームネットワーク 303 のユーザが決済機関 91 に支払った金銭が、コンテンツプロバイダ 301a、301b およびサービスプロバイダ 310 の所有者に分配される。

上述したように、EMD システム 300b によれば、セキュアコンテナ 304c 内に格納されたコンテンツファイル CFa、CFb の権利書データ 106a、106b は、コンテンツプロバイダ 301a、301b が作成したものをそのまま用いるため、SAM305₁ ~ 305₄ 内において、権利書データ 106a、106b に基づいて、コンテンツファイル CFa、CFb についての権利処理が

コンテンツプロバイダ 301a, 301b の意向に沿って確実に行われる。

なお、図 98 に示す第 2 変形例では、2 個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。

また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

第 2 実施形態の第 3 変形例

図 99 は、第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、EMD サービスセンタ 302 が決済機関 91 に対して、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の決済を行う場合を例示したが、本発明では、例えば、図 99 に示すように、EMD サービスセンタ 302 において、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301 のための決済請求権データ 152c と、サービスプロバイダ 310 のための決済請求権データ 152s とを作成し、これらをそれぞれコンテンツプロバイダ 301 およびサービスプロバイダ 310 に送信するようにしてもよい。

この場合には、コンテンツプロバイダ 301 は、決済請求権データ 152c を用いて、ペイメントゲートウェイ 90a を介して決済機関 91a に決済を行う。また、サービスプロバイダ 310 は、決済請求権データ 152s を用いて、ペイメントゲートウェイ 90b を介して決済機関 91b に決済を行う。

第 2 実施形態の第 4 変形例

図 100 は、第 2 実施形態の第 4 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、例えば現行のインターネットのようにサービスプロバイダ 310 が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ 310 が課金機能を有している場合には、CA モジュール 311 において、セキュアコンテナ 304 に関するサービスプロバ

イダ310のサービスに対しての利用履歴データ308sを作成してサービスプロバイダ310に送信する。

そして、サービスプロバイダ310は、利用履歴データ308sに基づいて、課金処理を行って決済請求権データ152sを作成し、これを用いてペイメントゲートウェイ90bを介して決済機関91bに決済を行う。

一方、SAM305₁～305₄は、セキュアコンテナ304に関するコンテンツプロバイダ301の権利処理に対しての利用履歴データ308cを作成し、これをEMDサービスセンタ302に送信する。

EMDサービスセンタ302は、利用履歴データ308cに基づいて、決済請求権データ152cを作成し、これをコンテンツプロバイダ301に送信する。

コンテンツプロバイダ301は、決済請求権データ152cを用いて、ペイメントゲートウェイ90aを介して決済機関91aに決済を行う。

第2実施形態の第5変形例

上述した実施形態では、図72に示すように、EMDサービスセンタ302のユーザ嗜好フィルタ生成部901において、SAM305₁などから受信した利用履歴データ308に基づいて、ユーザ嗜好フィルタデータ903を生成する場合を例示したが、例えば、図78に示すSAM305₁などの利用監視部186で生成されてリアルタイムにEMDサービスセンタ302に送信された利用制御状態データ166に基づいて、ユーザ嗜好フィルタ生成部901においてユーザ嗜好フィルタデータ903を生成してもよい。

第2実施形態の第6変形例

コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄は、それぞれ自らの公開鍵データK_{CP, P}、K_{SP, P}、K_{SAM1, P}～K_{SAM4, P}の他に、自らの秘密鍵データK_{CP, S}、K_{SP, S}、K_{SAM1, S}～K_{SAM4, S}をEMDサービスセンタ302に登録してもよい。

このようにすることで、EMDサービスセンタ302は、緊急時に、国家あるいは警察機関などからの要請に応じて、秘密鍵データ $K_{CP, S}$ 、 $K_{SP, S}$ 、 $K_{SAM1, S}$ ～ $K_{SAM4, S}$ を用いて、コンテンツプロバイダ301とサービスプロバイダ310との間の通信、サービスプロバイダ310とSAM305₁～305₄との間の通信、並びにユーザホームネットワーク303内でのSAM305₁～305₄相互間での通信のうち対象となる通信を盗聴することが可能になる。

また、SAM305₁～305₄については、出荷時に、EMDサービスセンタ302によって秘密鍵データ $K_{SAM1, S}$ ～ $K_{SAM4, S}$ を生成し、これをSAM305₁～305₄に格納すると共にEMDサービスセンタ302が保持（登録）するようにしてもよい。

第2実施形態の第7変形例

上述した実施形態では、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データ CER_{CP} 、 CER_{SP} 、 CER_{SAM1} ～ CER_{SAM4} を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。

例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データ CER_{CP} 、 CER_{SP} 、 CER_{SAM1} ～ CER_{SAM4} を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。

また、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が、通信時に、EMDサービスセンタ302から公開鍵証明書データ CER_{CP} 、 CER_{SP} 、 CER_{SAM1} ～ CER_{SAM4} を取得してもよい。

図101は、公開鍵証明書データの取得（入手）ルートの形態を説明するため

の図である。

なお、図101において、図59と同じ符号を付した構成要素は、前述した同一符号の構成要素と同じである。また、ユーザホームネットワーク303aは、前述したユーザホームネットワーク303と同じである。ユーザホームネットワーク303bでは、IEEE1394シリアルバスであるバス191を介してSAM305₁～305₄を接続している。

コンテンツプロバイダ301がサービスプロバイダ310の公開鍵証明書データCER_{sp}を取得する場合には、例えば、通信に先立ってサービスプロバイダ310からコンテンツプロバイダ301に公開鍵証明書データCER_{sp}を送信する場合(図101中(3))と、コンテンツプロバイダ301がEMDサービスセンタ302から公開鍵証明書データCER_{sp}を取り寄せる場合(図101中(1))とがある。

また、サービスプロバイダ310がコンテンツプロバイダ301の公開鍵証明書データCER_{cp}を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ301からサービスプロバイダ310に公開鍵証明書データCER_{cp}を送信する場合(図101中(2))と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データCER_{cp}を取り寄せる場合(図101中(4))とがある。

また、サービスプロバイダ310がSAM305₁～305₄の公開鍵証明書データCER_{sam1}～CER_{sam4}を取得する場合には、例えば、通信に先立ってSAM305₁～305₄からサービスプロバイダ310に公開鍵証明書データCER_{sam1}～CER_{sam4}を送信する場合(図101中(6))と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データCER_{sam1}～CER_{sam4}を取り寄せる場合(図101中(4))とがある。

また、SAM305₁～305₄がサービスプロバイダ310の公開鍵証明書データCER_{sp}を取得する場合には、例えば、通信に先立ってサービスプロバイ

ダ310からSAM305₁～305₄に公開鍵証明書データCER_{SP}を送信する場合(図101中(5))と、SAM305₁～305₄がEMDサービスセンタ302から公開鍵証明書データCER_{SP}を取り寄せる場合(図101中(7)など)とがある。

また、SAM305₁がSAM305₂の公開鍵証明書データCER_{SAM2}を取得する場合には、例えば、通信に先立ってSAM305₂からSAM305₁に公開鍵証明書データCER_{SAM2}を送信する場合(図101中(8))と、SAM305₁がEMDサービスセンタ302から公開鍵証明書データCER_{SAM2}を取り寄せる場合(図101中(7)など)とがある。

また、SAM305₂がSAM305₁の公開鍵証明書データCER_{SAM1}を取得する場合には、例えば、通信に先立ってSAM305₁からSAM305₂に公開鍵証明書データCER_{SAM1}を送信する場合(図101中(9))と、SAM305₂が自らEMDサービスセンタ302から公開鍵証明書データCER_{SAM1}を取り寄せる場合と、SAM305₁が搭載されたネットワーク機器を介して公開鍵証明書データCER_{SAM1}を取り寄せる場合(図101中(7)、(8))とがある。

また、SAM305₄がSAM305₁₃の公開鍵証明書データCER_{SAM13}を取得する場合には、例えば、通信に先立ってSAM305₁₃からSAM305₄に公開鍵証明書データCER_{SAM13}を送信する場合(図101中(12))と、SAM305₄が自らEMDサービスセンタ302から公開鍵証明書データCER_{SAM13}を取り寄せる場合(図101中(10))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCER_{SAM13}を取り寄せる場合とがある。

また、SAM305₁₃がSAM305₄の公開鍵証明書データCER_{SAM4}を取得する場合には、例えば、通信に先立ってSAM305₄からSAM305₁₃に公開鍵証明書データCER_{SAM4}を送信する場合(図101中(11))と、SA

M305₁が自らEMDサービスセンタ302から公開鍵証明書データCER_{SA}_{M4}を取り寄せる場合(図101中(13))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCER_{SA}_{M4}を取り寄せる場合とがある。

第2実施形態における公開鍵証明書破棄リスト(データ)の取り扱い

第2実施形態では、EMDサービスセンタ302において、不正行為などに用いられたコンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データCRL(Certificate Revocation List)を、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄に送信する。

なお、公開鍵証明書破棄データCRLは、EMDサービスセンタ302の他に、例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄において生成してもよい。

まず、EMDサービスセンタ302が、コンテンツプロバイダ301の公開鍵証明書データCER_{CP}を無効にする場合について説明する。

図102に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{CP}を無効にすることを示す公開鍵証明書破棄データCRL₁をサービスプロバイダ310に送信する(図102中(1))。サービスプロバイダ310は、コンテンツプロバイダ301から入力した署名データを検証する際に、公開鍵証明書破棄データCRL₁を参照して公開鍵証明書データCER_{CP}の有効性を判断し、有効であると判断した場合に公開鍵データK_{CP}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ301からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₁を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM305₁に送信する(図102中(1))、(2))。SAM305₁は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ301の署名データを検証する際に、公開鍵証明書破棄データCRL₁を参照して公開鍵証明書データCER_{op}の有効性を判断し、有効であると判断した場合に公開鍵データK_{op}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₁を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図102中(3))。

次に、EMDサービスセンタ302が、サービスプロバイダ310の公開鍵証明書データCER_{sp}を無効にする場合について説明する。

図103に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{sp}を無効にすることを示す公開鍵証明書破棄データCRL₂をコンテンツプロバイダ301に送信する(図103中(1))。コンテンツプロバイダ301は、サービスプロバイダ310から入力した署名データを検証する際に、公開鍵証明書破棄データCRL₂を参照して公開鍵証明書データCER_{sp}の有効性を判断し、有効であると判断した場合に公開鍵データK_{sp}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ310からのデータを無効にする。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₂を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM305₁に送信する(図103中(2))。SAM305₁は、サービスプロバイダ310

0から入力したセキュアコンテナ内に格納されたサービスプロバイダ310の署名データを検証する際に、公開鍵証明書破棄データCRL₂を参照して公開鍵証明書データCER_{sp}の有効性を判断し、有効であると判断した場合に公開鍵データK_{sp, p}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₂の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₂は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₂を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図103中(3))。

次に、EMDサービスセンタ302が、例えばSAM305₂の公開鍵証明書データCER_{sam2}を無効にする場合について説明する。

図104に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{sam2}を無効にすることを示す公開鍵証明書破棄データCRL₂をコンテンツプロバイダ301に送信する(図104中(1))。コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₂をサービスプロバイダ310に送信する。サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM305₁に公開鍵証明書破棄データCRL_{sam1}を送信する(図104中(1))。SAM305₁は、SAM305₂から入力したデータに付加されたSAM305₂の署名データを検証する際に、公開鍵証明書破棄データCRL₂を参照して公開鍵証明書データCER_{sam2}の有効性を判断し、有効であると判断した場合に公開鍵データK_{sam2, p}を用いた署名検証を行い、無効であると判断した場

合に当該署名検証を行わずに当該データを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₁の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₁は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

EMDサービスセンタ302は、公開鍵証明書破棄データCRL₁をサービスプロバイダ310を介してSAM305₁に送信してもよい(図104中(1)、(2))。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₁を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図104中(3))。

また、EMDサービスセンタ302は、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₁を作成し、これを保管する。

また、ユーザホームネットワーク303は、バス191に接続されているSAMのSAM登録リストSRLを作成し、これをEMDサービスセンタ302に送信する(図105中(1))。

EMDサービスセンタ302は、SAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₁によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定して新たなSAM登録リストSRLを作成する。

次に、EMDサービスセンタ302は、当該生成したSAM登録リストSRLをSAM305₁に送信する(図105中(1))。

SAM305₁は、他のSAMと通信を行う際に、SAM登録リストSRLの

破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₁を作成し、これをコンテンツプロバイダ301に送信する(図105中(2))。

コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₁をサービスプロバイダ310に送信する(図105中(2))。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₁をSAM305₁に送信する(図105中(2))。

SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305_nのうち、公開鍵証明書破棄データCRL₁によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₂を作成し、これをサービスプロバイダ310に送信する(図105中(3))。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₂をSAM305₁に送信する(図105中(3))。

SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305_nのうち、公開鍵証明書破棄データCRL₂によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リス

トSRLの破棄フラグを参照して、署名データの検証の有無および通信を許可するか否かを決定する。

EMDサービスセンタ302の役割等

図106は、図59に示すEMDサービスセンタ（クリアリングハウス）302の機能を権利管理用クリアリングハウス950と、電子決済用クリアリングハウス951とに分割した場合のEMDシステムの構成図である。

当該EMDシステムでは、電子決済用クリアリングハウス951において、ユーザホームネットワーク303a、303bのSAMからの利用履歴データ308に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ301およびサービスプロバイダ310の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ90を介して決済機関91において決済を行う。

また、権利管理用クリアリングハウス950は、電子決済用クリアリングハウス951からの決済通知に応じたコンテンツプロバイダ301およびサービスプロバイダ310の決済レポートを作成し、それらをコンテンツプロバイダ301およびコンテンツプロバイダ301に送信する。

また、コンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データKcの登録（権威化）などを行う。

なお、図107に示すように、権利管理用クリアリングハウス950と電子決済用クリアリングハウス951とを単体の装置内に収納すると、図59に示すEMDサービスセンタ302となる。

また、本発明は、例えば、図108に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス960の機能を設け、権利管理用クリアリングハウス960において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてサービスプロバイダ310の決済請求権データを作成し、これをサービスプロバイダ310に送信してもよい。この場合には、サービスプロバイダ310は、自らの課金システムを電子決済用クリア

リングハウス 961 として利用し、権利管理用クリアリングハウス 960 からの決済請求権データに基づいて決済を行う。

また、本発明は、例えば、図 109 に示すように、EMD サービスセンタ 302 に、権利管理用クリアリングハウス 970 の機能を設け、権利管理用クリアリングハウス 970 において、権利書データ 106 の登録などを行うと共に、SAM からの利用履歴データ 308 に基づいてコンテンツプロバイダ 301 の決済請求権データを作成し、これをコンテンツプロバイダ 301 に送信してもよい。この場合には、コンテンツプロバイダ 301 は、自らの課金システムを電子決済用クリアリングハウス 961 として利用し、権利管理用クリアリングハウス 970 からの決済請求権データに基づいて決済を行う。

また、本発明は、例えば、図 110 に示すように、コンテンツプロバイダ 301 内に、前述した権利管理用クリアリングハウス 970 および電子決済用クリアリングハウス 971 の機能を備えるようにしてもよい。

この場合には、コンテンツプロバイダ 301 は、自らの課金システムを電子決済用クリアリングハウス 961 として利用し、権利管理用クリアリングハウス 970 において生成した決済請求権データに基づいて、決済機関 91 に対して自ら決済を行う。

第 2 実施形態の第 8 変形例

上述した第 2 実施形態では、図 59 に示す EMD システム 300 において、コンテンツプロバイダ 301 からサービスプロバイダ 310 に図 5 に示すフォーマットのセキュアコンテナ 104 を提供し、サービスプロバイダ 310 からユーザホームネットワーク 303 に図 65 に示すフォーマットのセキュアコンテナ 304 を配給する場合を例示した。

すなわち、上述した第 2 実施形態では、図 5 および図 65 に示すように、セキュアコンテナ 104 およびセキュアコンテナ 304 内に、それぞれ単数のコンテンツファイル CF と、当該コンテンツファイル CF に対応する単数のキーファ

ルKFを格納した場合を例示した。

本発明では、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ複数のコンテンツファイルCFと、当該複数のコンテンツファイルCFにそれぞれ対応する複数のキーファイルKFとを格納してもよい。

図111は、本変形例において、図59に示すコンテンツプロバイダ301からサービスプロバイダ310に提供されるセキュアコンテナ104aのフォーマットを説明するための図である。

図111に示すように、セキュアコンテナ104aには、コンテンツファイルCF₁、CF₂、CF₃、キーファイルKF₁、KF₂、KF₃、公開鍵証明書データCER_{CP}、署名データSIG_{200,CP}、SIG_{201,CP}、SIG_{202,CP}、SIG_{203,CP}、SIG_{204,CP}、SIG_{205,CP}、SIG_{1,ESC}が格納されている。

ここで、署名データSIG_{200,CP}、SIG_{201,CP}、SIG_{202,CP}、SIG_{203,CP}、SIG_{204,CP}、SIG_{205,CP}は、コンテンツプロバイダ301において、それぞれコンテンツファイルCF₁、CF₂、CF₃、キーファイルKF₁、KF₂、KF₃に対してハッシュ値を取り、コンテンツプロバイダ301の秘密鍵データK_{CP}を用いて生成される。

コンテンツファイルCF₁には、ヘッダ、メタデータMeta₁、コンテンツデータC₁、A/V伸長用ソフトウェアSoft₁および電子透かし情報モジュールWM₁が格納されている。

ここで、コンテンツデータC₁およびA/V伸長用ソフトウェアSoft₁は、コンテンツ鍵データK_Cを用いて暗号化されており、メタデータMeta₁および電子透かし情報モジュールWM₁は必要に応じてコンテンツ鍵データK_Cを用いて暗号化されている。

また、コンテンツデータC₁は、例えば、ATRAC3方式で圧縮されている。A/V伸長用ソフトウェアSoft₁は、ATRAC3方式の伸長用のソフトウェアである。

また、コンテンツファイルCF₁のヘッダには、例えば、図112に示すようにキーファイルKF₁およびコンテンツファイルCF₂にリンクすることを示すディレクトリ構造データDSD₁が含まれている。

コンテンツファイルCF₂には、ヘッダ、メタデータMeta₂、コンテンツデータC₂、A/V伸長用ソフトウェアSoft₂および電子透かし情報モジュールWM₂が格納されている。

ここで、コンテンツデータC₂およびA/V伸長用ソフトウェアSoft₂は、コンテンツ鍵データKc₂を用いて暗号化されており、メタデータMeta₂および電子透かし情報モジュールWM₂は必要に応じてコンテンツ鍵データKc₂を用いて暗号化されている。

また、コンテンツデータC₂は、例えば、MPEG2方式で圧縮されている。A/V伸長用ソフトウェアSoft₂は、MPEG2方式の伸長用のソフトウェアである。

また、コンテンツファイルCF₂のヘッダには、例えば、図112に示すように、キーファイルKF₂およびコンテンツファイルCF₃にリンクすることを示すディレクトリ構造データDSD₂が含まれている。

コンテンツファイルCF₃には、ヘッダ、メタデータMeta₃、コンテンツデータC₃、A/V伸長用ソフトウェアSoft₃および電子透かし情報モジュールWM₃が格納されている。

ここで、コンテンツデータC₃およびA/V伸長用ソフトウェアSoft₃は、コンテンツ鍵データKc₃を用いて暗号化されており、メタデータMeta₃および電子透かし情報モジュールWM₃は必要に応じてコンテンツ鍵データKc₃を用いて暗号化されている。

また、コンテンツデータC₃は、例えば、JPEG方式で圧縮されている。A/V伸長用ソフトウェアSoft₃は、JPEG方式の伸長用のソフトウェアである。

また、コンテンツファイルCF₃のヘッダには、例えば、図112に示すように、キーファイルKF₃にリンクすることを示すディレクトリ構造データDSD₃が含まれている。

キーファイルKF₁には、ヘッダと、配信鍵データKD₁～KD₃を用いて暗号化されたコンテンツ鍵データKc₁、権利書データ106₁およびSAMプログラム・ダウンロード・コンテナSDC₁と、署名データSIG_{220, esc}とが格納されている。

キーファイルKF₂には、ヘッダと、配信鍵データKD₁～KD₃を用いて暗号化されたコンテンツ鍵データKc₂、権利書データ106₂およびSAMプログラム・ダウンロード・コンテナSDC₂と、署名データSIG_{221, esc}とが格納されている。

キーファイルKF₃には、ヘッダと、配信鍵データKD₁～KD₃を用いて暗号化されたコンテンツ鍵データKc₃、権利書データ106₃、およびSAMプログラム・ダウンロード・コンテナSDC₃と、署名データSIG_{222, esc}とが格納されている。

サービスプロバイダ310は、図112に示すセキュアコンテナ104aの配給を受けると、EMDサービスセンタ302の公開鍵データK_{esc, p}を用いて公開鍵証明書データCER_{es}の正当性を確認した後に、当該公開鍵証明書データCER_{es}に格納された公開鍵データK_{es, p}を用いて、署名データSIG_{200, cp}, SIG_{201, cp}, SIG_{202, cp}, SIG_{203, cp}, SIG_{204, cp}, SIG_{205, cp}の正当性、すなわちコンテンツファイルCF₁, CF₂, CF₃の作成者および送信者の正当性と、キーファイルKF₁, KF₂, KF₃の送信者の正当性を確認する。

また、コンテンツプロバイダ301は、公開鍵データK_{esc, p}を用いて、署名データSIG_{220, esc}, SIG_{221, esc}, SIG_{222, esc}の正当性、キーファイルKF₁, KF₂, KF₃の作成者の正当性を確認する。

そして、サービスプロバイダ310は、コンテンツファイルCF₁、CF₂、CF₃の販売価格を示すプライスタグデータ312₁、312₂、312₃を作成する。

また、サービスプロバイダ310は、秘密鍵データK_{SP, S}を用いて、プライスタグデータ312₁、312₂、312₃の署名データSIG_{220, SP}、SIG_{221, SP}、SIG_{222, SP}を作成する。

また、サービスプロバイダ310は、秘密鍵データK_{SP, S}を用いて、コンテンツファイルCF₁、CF₂、CF₃、KF₁、KF₂、KF₃の署名データSIG_{210, SP}、SIG_{211, SP}、SIG_{212, SP}、SIG_{213, SP}、SIG_{214, SP}、SIG_{215, SP}を作成する。

次に、サービスプロバイダ310は、図114に示すセキュアコンテナ304aを作成する。

サービスプロバイダ310は、図114に示すセキュアコンテナ304aをユーザホームネットワーク303に配給する。

ユーザホームネットワーク303では、SAM305₁～305₄において、セキュアコンテナ304aに格納された全ての署名データの正当性を確認した後、コンテンツデータC₁、C₂、C₃についての権利処理を、ディレクトリ構造データDSD₁～DSD₃に示されるリンク状態に応じて、それぞれキーファイルKF₁、KF₂、KF₃に基づいて行う。

また、上述した第8変形例では、セキュアコンテナ304において、単数のサービスプロバイダ310から提供を受けた複数のコンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃を単数のセキュアコンテナ304aに格納してユーザホームネットワーク303に配給する場合を例示したが、図98に示すように、複数のコンテンツプロバイダ301a、301bから提供を受けた複数のコンテンツファイルCFを、単数のセキュアコンテナに格納してユーザホームネットワーク303に配給してもよい。

また、セキュアコンテナ104、304内には、例えば、図113に示すように、ATRAC3で圧縮された楽曲（音声）データを格納したコンテンツファイルCF₁、MPEG2で圧縮されたビデオクリップデータを格納したコンテンツファイルCF₂、JPEGで圧縮されたジャケット（静止画）データを格納したコンテンツファイルCF₃、テキスト形式の歌詞データを格納したコンテンツファイルCF₄並びにテキスト形式のライナーノーツデータを格納したコンテンツファイルCF₅と、それぞれに対応したキーファイルKF₁、KF₂、KF₃、KF₄、KF₅とを格納してもよい。

この場合にも、同様に、コンテンツファイルCF₁～CF₅のディレクトリ構造データによって、コンテンツファイルCF₁～CF₅相互間のリンクと、コンテンツファイルCF₁～CF₅とキーファイルKF₁～KF₅との間のそれぞれのリンクとが確立される。

なお、本実施形態におけるセキュアコンテナ内に複数のコンテンツデータを格納する場合（コンポジット型の場合）のデータフォーマットの概念は、例えば、図115あるいは図116に示される。

なお、図111に示すフォーマットは、前述した第1実施形態において、図1に示すコンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を送信する場合にも同様に適用できる。

第2実施形態の第9変形例

上述した実施形態では、コンテンツファイルCFおよびキーファイルKFをディレクトリ構造でセキュアコンテナ104、304に格納してコンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁～305₄に送信する場合を例示したが、コンテンツファイルCFおよびキーファイルKFを、別々にコンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁～305₄に送信してもよい。

これには、例えば、以下に示す第1の手法と第2の手法とがある。

第1の手法では、図117に示すように、コンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁～305₄に、コンテンツファイルCFおよびキーファイルKFを別々に送信する。

また、第2の手法では、図118に示すように、コンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁～305₄にコンテンツファイルCFを送信し、EMDサービスセンタ302からSAM305₁～305₄にキーファイルKFを送信する。当該キーファイルKFの送信は、例えば、SAM305₁～305₄のユーザが、コンテンツデータCの購入形態を決定しようとするときに、EMDサービスセンタ302からSAM305₁～305₄に送信される。

上述した第1の手法および第2の手法を採用する場合には、例えば、関連するコンテンツファイルCF相互間と、コンテンツファイルCFとそれに対応するキーファイルKFとの間を、コンテンツファイルCFおよびキーファイルKFの少なくとも一方のヘッダに格納されたハイパーリンクデータHLを用いてリンク関係を確立する。SAM105₁～105₄では、当該リンク関係に基づいて、コンテンツデータCの権利処理および利用を行う。

また、上述した第2実施形態では、コンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106などの鍵データとをそれぞれファイル形式にして、コンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁～305₄に送信する場合を例示したが、これらは、相互間でのリンク関係が確立できれば、必ずしもファイル形式にする必要はない。

例えば、図119に示すように、コンテンツデータC、メタデータMeta、A/V伸長用ソフトウェアSoft、電子透かし情報モジュールWM、キーフ

ファイルKF、プライスタグデータ312および、公開鍵証明書データCER_{cp}、CER_{sp}を別々に、コンテンツプロバイダ301およびEMDサービスセンタ302からSAM305₁～305₄に送信してもよい。

この場合には、図119に示すように、コンテンツデータC、メタデータMeta、A/V伸長用ソフトウェアSoft、電子透かし情報モジュールWM、キーファイルKF、プライスタグデータ312、公開鍵証明書データCER_{cp}、CER_{sp}が、ハイパーリンクデータHLによってリンクされる。

ここで、ハイパーリンクデータHLは、例えば、配信用鍵データKD₁～KD₄で暗号化されて送信される。

なお、本変形例において、コンテンツファイルCFおよびキーファイルKFのフォーマットは、例えば、図5(A)、(B)に示すものが採用される。また、この場合に、コンテンツファイルCFおよびキーファイルKFと共に、それらの署名データSIG_{s, cp}、SIG_{s, sp}を送信することが好ましい。

第2実施形態の第10変形例

上述した実施形態では、セキュアコンテナ104内において、コンテンツファイルCFおよびキーファイルKFを別々に設けた場合を例示したが、例えば、図120に示すように、セキュアコンテナ104、304内において、コンテンツファイルCF内にキーファイルKFを格納するようにしてもよい。

この場合に、キーファイルKFを格納したコンテンツファイルCFに対して、コンテンツプロバイダ301の秘密鍵データK_{cp, s}による署名データ、並びにサービスプロバイダ310の秘密鍵データK_{sp, s}による署名データが付される。

第2実施形態の第11変形例

上述した実施形態では、コンテンツデータCをコンテンツファイルCFに格納し、コンテンツ鍵データKcおよび権利書データ106をキーファイルKF内に格納してコンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁などに送信する場合を例示したが、

コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106の少なくとも一つをファイル形式を採用せずにコンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305、などに、通信プロトコルに依存しない形式で送信してもよい。

例えば、図121に示すように、コンテンツプロバイダ301において、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFとを格納したセキュアコンテナ104sを作成し、セキュアコンテナ104sをサービスプロバイダ310に通信プロトコルに依存しない形式で送信する。そして、サービスプロバイダ310において、セキュアコンテナ104sに格納されたコンテンツデータCおよびキーファイルKFにブライスタグデータ312を加えてセキュアコンテナ304sを作成し、セキュアコンテナ304sをSAM305、などに通信プロトコルに依存しない形式で送信してもよい。

また、図122に示すように、コンテンツプロバイダ301からサービスプロバイダ310に、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFとを通信プロトコルに依存しない形式で個別に送信する。そして、サービスプロバイダ310からSAM305、などに、コンテンツデータC、キーファイルKFおよびブライスタグデータ312を通信プロトコルに依存しない形式で個別に送信する。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと同一経路で送信する。

また、図123に示すように、コンテンツプロバイダ301からサービスプロバイダ310に、コンテンツ鍵データKcで暗号化されたコンテンツデータCを通信プロトコルに依存しない形式で送信し、サービスプロバイダ310からSAM305、などにコンテンツデータCおよびブライスタグデータ312を通信プロトコルに依存しない形式で送信する。また、暗号化されたコンテンツ鍵データ

Kcおよび暗号化された権利書データ106などを含むキーファイルKFをEMDサービスセンタ302からSAM305、などに送信してもよい。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと別経路で送信する。

また、図124に示すように、コンテンツプロバイダ301からサービスプロバイダ310に、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106とを、通信プロトコルに依存しない形式で送信する。また、サービスプロバイダ310からSAM305、などに、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106、並びにプライスタグデータ312を送信する。すなわち、コンテンツデータC、コンテンツ鍵データKc、権利書データ106およびプライスタグデータ312をファイル形式にしないで、同一経路で送信する。

また、図125に示すように、コンテンツプロバイダ301からサービスプロバイダ310に、コンテンツ鍵データKcで暗号化されたコンテンツデータCを、通信プロトコルに依存しない形式で送信する。そして、サービスプロバイダ310からSAM305、などに、コンテンツデータCおよびプライスタグデータ312を、通信プロトコルに依存しない形式で送信する。また、EMDサービスセンタ302からSAM305、などにコンテンツ鍵データKcおよび権利書データ106を送信する。すなわち、コンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106とをファイル形式にしないで、別経路で送信する。

第2実施形態の第12変形例

前述した図59に示すEMDシステム300では、例えば、図126に示すように、ユーザホームネットワーク303がサービスプロバイダ310から受信したセキュアコンテナ304に応じたセキュアコンテナ304Aを、ユーザホームネットワーク303aのSAMからの要求S303aに応じて、ユーザホームネ

ットワーク 303a に配給してもよい。

この場合には、ユーザホームネットワーク 303 の SAM が、前述した第 2 実施形態で説明したサービスプロバイダ 310 と同様の役割を果たすと考えることができる。

この場合に、ユーザホームネットワーク 303a の SAM は、独自にプライスタグデータ 312 を新たに設定できる。

そして、ユーザホームネットワーク 303a の SAM においてコンテンツデータ C の購入形態が決定され、それに応じた利用履歴データ 304a などがユーザホームネットワーク 303a の SAM から EMD サービスセンタ 302 に送信される。

EMD サービスセンタ 302 では、利用履歴データ 304a に基づいて、コンテンツプロバイダ 301、サービスプロバイダ 310、ユーザホームネットワーク 303 のユーザに、ユーザホームネットワーク 303a のユーザが支払った金銭を分配するための決済処理を行う。

なお、本実施形態におけるセキュアコンテナのファイル包括大小関係は、図 127 に示すように表現できる。

第 3 実施形態

図 128 は本発明の第 3 実施形態の EMD システムを説明するための図、図 129 は図 128 に示す EMD サービスセンタの機能ブロック図である。

図 129 において、前述した第 1 実施形態および第 2 実施形態で用いた符号と同じ符号を付した構成要素は、これらの実施形態で説明した同一符号の構成要素と同じである。

本実施形態の EMD システムでは、コンテンツプロバイダ 301 は EMD サービスセンタ 302 にマスタソース（コンテンツデータ）S111 などを送り、EMD サービスセンタ 302 において例えば図 5（A）に示すコンテンツファイル CF を作成する。

また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータS111のコンテンツID、コンテンツ鍵データKc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容）、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格SRPを送り、EMDサービスセンタ302において図5（B）に示すキーファイルKFを作成する。

また、EMDサービスセンタ302は、作成したコンテンツファイルCFをCFデータベース802aに格納し、個々のコンテンツファイルCFにグローバルユニークなコンテンツIDを付して、これらを一元的に管理する。また、EMDサービスセンタ302は、キーファイルKFをKFデータベース153aに格納し、これについてもコンテンツIDを用いて一元的に管理する。

EMDサービスセンタ302における処理を図129を参照して説明する。

EMDサービスセンタ302は、コンテンツプロバイダ301から受け取ったマスタソースS111をコンテンツマスタソースデータベース801に格納する。

次に、電子透かし情報付加部112において、コンテンツプロバイダ301から受け取った電子透かし管理情報が示す電子透かし情報を、コンテンツマスタソースデータベース801から読み出したマスタソースS111に埋め込んでコンテンツデータS112を生成する。

次に、圧縮部113において、コンテンツデータS112を圧縮してコンテンツデータS113を生成する。

コンテンツデータS112は、伸長部116において伸長された後に、聴感検査部123において聴覚検査が行われ、必要であれば、電子透かし情報付加部112において電子透かし情報が再び埋め込まれる。

次に、暗号化部114において、コンテンツデータS113がコンテンツ鍵デ

ータKcを用いて暗号化されてコンテンツデータS114が生成される。

次に、CF作成部802において、コンテンツデータS114などを格納した図5(A)に示すコンテンツファイルCFが作成され、コンテンツファイルCFがCFデータベース802aに格納される。

また、EMDサービスセンタ302では、KF作成部153において、図5(B)に示すキーファイルKFを作成し、キーファイルKFをKFデータベース153aに格納する。

次に、セキュアコンテナ作成部804において、CFデータベース802aから読み出したコンテンツファイルCFと、KFデータベース153aから読み出したキーファイルKFとを格納したセキュアコンテナ806が作成され、セキュアコンテナ806がセキュアコンテナデータベース805に格納される。

その後、セキュアコンテナデータベース805が、サービスプロバイダ310によってアクセスされて、セキュアコンテナ806がサービスプロバイダ310に供給される。

次に、サービスプロバイダ310は、セキュアコンテナ806に格納されたコンテンツファイルCFおよびキーファイルKFと、コンテンツデータの販売価格を示すプライスタグデータ312とを格納したセキュアコンテナ807を作成する。

そして、サービスプロバイダ310は、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいはROM型などの記録媒体に記録してセキュアコンテナ807をユーザホームネットワーク303に配給する。

ユーザホームネットワーク303では、オンラインの場合にはCAモジュール311を介してセキュアコンテナ807がSAM305、などに提供され、SAM305、などにおいて、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKD₁～KD_nなどを用いて復号され、復号された権利書データ106に基づいて、コンテンツファイルC

Fに格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、SAM305₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。

また、ユーザホームネットワーク303のSAM305₂から、ユーザホームネットワーク303aのSAM305₁₂にセキュアコンテナ807が配給された場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。

また、図128に示す例では、EMDサービスセンタ302からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送信する場合（イン・バンドの場合）を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。

また、図130に示すように、EMDサービスセンタ302において作成したコンテンツファイルCFをサービスプロバイダ310に供給し、サービスプロバイダ310がコンテンツファイルCFをユーザホームネットワーク303に供給すると共に、EMDサービスセンタ302において作成したキーファイルKFをEMDサービスセンタ302からユーザホームネットワーク303、303aのSAM305₂、SAM305₁₂に供給してもよい。

第4実施形態

図131は本発明の第4実施形態のEMDシステムを説明するための図である

。

本実施形態のEMDシステムでは、コンテンツプロバイダ301は例えば図5(A)に示すコンテンツファイルCFを作成し、これをEMDサービスセンタ302に送る。

また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データKc、電子透かし管理情報(コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報)、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格SRPを送り、EMDサービスセンタ302において図5(B)に示すキーファイルKFを作成する。

また、EMDサービスセンタ302は、コンテンツファイルCFをCFデータベース802aに格納し、個々のコンテンツファイルCFにグローバルユニークなコンテンツIDを付して、これらを一元的に管理する。また、EMDサービスセンタ302は、作成したキーファイルKFをKFデータベース153aに格納し、これについてもコンテンツIDを用いて一元的に管理する。

また、EMDサービスセンタ302では、CFデータベース802aから読み出したコンテンツファイルCFと、KFデータベース153aから読み出したキーファイルKFとを格納したセキュアコンテナ806が作成され、セキュアコンテナ806がセキュアコンテナデータベースに格納される。

その後、セキュアコンテナデータベースが、サービスプロバイダ310によってアクセスされて、セキュアコンテナ806がサービスプロバイダ310に供給される。

次に、サービスプロバイダ310は、セキュアコンテナ806に格納されたコンテンツファイルCFおよびキーファイルKFと、コンテンツデータの販売価格を示すプライスタグデータ312とを格納したセキュアコンテナ807を作成す

る。

そして、サービスプロバイダ310は、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいはROM型などの記録媒体に記録してセキュアコンテナ807をユーザホームネットワーク303に配給する。

ユーザホームネットワーク303では、オンラインの場合にはCAモジュール311を介してセキュアコンテナ807がSAM305₁などに提供され、SAM305₁などにおいて、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKD₁～KD_nなどを用いて復号され、復号された権利書データ106に基づいて、コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、SAM305₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。

また、ユーザホームネットワーク303のSAM305₂から、ユーザホームネットワーク303aのSAM305₁₂にセキュアコンテナ807が配給された場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。

また、図131に示す例では、EMDサービスセンタ302からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送信する場合（イン・バンドの場合）を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・

オブ・バンドの場合)。

また、図132に示すように、コンテンツファイルCFをEMDサービスセンタ302からサービスプロバイダ310に供給し、サービスプロバイダ310がコンテンツファイルCFをユーザホームネットワーク303に供給すると共に、EMDサービスセンタ302において作成したキーファイルKFをEMDサービスセンタ302からユーザホームネットワーク303、303aのSAM305₁、SAM305₁₂に供給してもよい。

第5実施形態

図133は本発明の第5実施形態のEMDシステムを説明するための図である。

本実施形態のEMDシステムでは、コンテンツプロバイダ301は例えば図5(A)に示すコンテンツファイルCFを作成する。

また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データKc、電子透かし管理情報(コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報)、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格SRPを送り、EMDサービスセンタ302において図5(B)に示すキーファイルKFを作成する。

EMDサービスセンタ302は、作成したキーファイルKFをコンテンツプロバイダ301に送る。

また、EMDサービスセンタ302は、KFデータベース153aにキーファイルKFを格納し、個々のコンテンツデータに割り当てられたコンテンツIDを用いてキーファイルKFを一元的に管理する。このとき、コンテンツIDは、例えば、EMDサービスセンタ302によって作成され、複数のコンテンツプロバイダ301が提供するコンテンツデータの全てを対象としてグローバルユニーク

に決定される。

次に、コンテンツプロバイダ 301 において、作成したコンテンツファイル C F と、EMD サービスセンタ 302 から受けたキーファイル K F とを格納したセキュアコンテナ 821 が作成され、セキュアコンテナ 821 が共通データベース 820 に格納される。

共通データベース 820 において、複数のコンテンツプロバイダ 301 が提供したセキュアコンテナ 821 が、コンテンツ ID を用いて一元的に管理される。

サービスプロバイダ 310 は、例えば、コンテンツ ID を用いて共通データベース 820 をブランジング（検索）して、所望のセキュアコンテナ 821 を共通データベース 820 から受けて、セキュアコンテナ 821 に、コンテンツの販売価格を示すプライスタグデータ 312 などをさらに格納したセキュアコンテナ 822 を作成し、セキュアコンテナ 822 をユーザホームネットワーク 303 に配給する。

ユーザホームネットワーク 303 では、オンラインの場合には C A モジュール 311 を介してセキュアコンテナ 822 が S A M 305₁ などに提供され、S A M 305₁ などにおいて、キーファイル K F に格納されたコンテンツ鍵データ K c および権利書データ 106 などが配信用鍵データ K D₁ ~ K D_n などを用いて復号され、復号された権利書データ 106 に基づいて、コンテンツファイル C F に格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、S A M 305₁ などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ 308 が生成され、利用履歴データ 308 が EMD サービスセンタ 302 に送信される。

また、ユーザホームネットワーク 303 の S A M 305₂ から、ユーザホームネットワーク 303 a の S A M 305₁₂ にセキュアコンテナ 822 が配給された場合には、S A M 305₁₂ において S A M 305₂ と同様の処理が行われ、S A

M305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。

また、図133に示す例では、コンテンツプロバイダ301から共通データベース820、共通データベース820からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。

また、図134に示すように、コンテンツプロバイダ301から共通データベース820にコンテンツファイルCFを格納し、サービスプロバイダ310が共通データベース820からコンテンツファイルCFを得ると共に、EMDサービスセンタ302からサービスプロバイダ310にキーファイルKFを送るようにしてもよい。この場合には、サービスプロバイダ310は、共通データベース820から得たコンテンツファイルCFと、EMDサービスセンタ302から得たキーファイルKFと、プライスタグデータ312とを格納してセキュアコンテナ822を作成する。

共通データベース820は、複数のコンテンツプロバイダ301が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツIDを用いて、コンテンツファイルCFを一元的に管理する。

また、図135に示すように、EMDサービスセンタ302が作成したキーファイルKFを、ユーザホームネットワーク303、303aのSAM305₁、305₁₂などに送るようにしてもよい。この場合には、サービスプロバイダ310は、コンテンツファイルCFをユーザホームネットワーク303に配給する。

プライスタグデータ 312 は、サービスプロバイダ 310 がユーザホームネットワーク 303 に配給してもよいし、EMD サービスセンタ 302 がユーザホームネットワーク 303, 303a に配給してもよい。

第 6 実施形態

図 136 は本発明の第 6 実施形態の EMD システムを説明するための図である。

本実施形態の EMD システムは、前述した図 133 に示す EMD システムと比較すると、複数の EMD サービスセンタ 302 を有し、コンテンツプロバイダ 301 がそれぞれ対応する EMD サービスセンタ 302 との間で課金処理などを行うことを特徴としている点が異なり、それ以外の点は略同じである。

コンテンツプロバイダ 301 は例えば図 5 (A) に示すコンテンツファイル CF を作成する。

また、コンテンツプロバイダ 301 は、複数の EMD サービスセンタ 302 のうち自らが選択した（あるいは予め決められた）一の EMD サービスセンタ 302 に、コンテンツデータのコンテンツ ID、コンテンツ鍵データ Kc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報）、コンテンツプロバイダ 301 の識別子 CP_ID、コンテンツデータを提供するサービスプロバイダ 310 の識別子 SP_ID、コンテンツデータの卸売価格 SRP を送り、EMD サービスセンタ 302 において図 5 (B) に示すキーファイル KF を作成する。

EMD サービスセンタ 302 は、作成したキーファイル KF を、対応するコンテンツプロバイダ 301 に送る。

また、EMD サービスセンタ 302 は、KF データベース 153a にキーファイル KF を格納し、個々のコンテンツデータに割り当てられたコンテンツ ID を用いてキーファイル KF を一元的に管理する。このとき、コンテンツ ID は、例えば、EMD サービスセンタ 302 によって作成され、共通データベース 830

に格納される全てのセキュアコンテナ 831 に対応するコンテンツデータを対象としてグローバルユニークに決定される。

次に、コンテンツプロバイダ 301 において、作成したコンテンツファイル C F と、EMD サービスセンタ 302 から受けたキーファイル K F とを格納したセキュアコンテナ 831 が作成され、セキュアコンテナ 831 が共通データベース 820 に格納される。

共通データベース 830 において、複数のコンテンツプロバイダ 301 が提供したセキュアコンテナ 831 が、コンテンツ ID を用いて一元的に管理される。

サービスプロバイダ 310 は、例えば、コンテンツ ID を用いて共通データベース 820 をブランジング（検索）して、所望のセキュアコンテナ 831 を共通データベース 820 から受けて、セキュアコンテナ 831 に、コンテンツの販売価格を示すプライスタグデータ 312 などをさらに格納したセキュアコンテナ 832 を作成し、セキュアコンテナ 832 をユーザホームネットワーク 303 に配給する。

ユーザホームネットワーク 303 では、オンラインの場合には C A モジュール 311 を介してセキュアコンテナ 832 が S A M 305₁ などに提供され、S A M 305₁ などにおいて、キーファイル K F に格納されたコンテンツ鍵データ K c および権利書データ 106 などが配信用鍵データ K D₁ ~ K D_n などを用いて復号され、復号された権利書データ 106 に基づいて、コンテンツファイル C F に格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、S A M 305₁ などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ 308 が生成され、利用履歴データ 308 が EMD サービスセンタ 302 に送信される。

また、ユーザホームネットワーク 303 の S A M 305₂ から、ユーザホームネットワーク 303 a の S A M 305₁₂ にセキュアコンテナ 832 が配給された

場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。

また、図136に示す例では、コンテンツプロバイダ301から共通データベース830、共通データベース830からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。

また、図137に示すように、コンテンツプロバイダ301から共通データベース830にコンテンツファイルCFを格納し、サービスプロバイダ310が共通データベース820からコンテンツファイルCFを得ると共に、EMDサービスセンタ302からサービスプロバイダ310にキーファイルKFを送るようにしてもよい。このとき、サービスプロバイダ310が得たコンテンツファイルCFを作成したコンテンツプロバイダ301に対応するEMDサービスセンタ302からサービスプロバイダ310にキーファイルKFが送られる。

サービスプロバイダ310は、共通データベース830から得たコンテンツファイルCFと、EMDサービスセンタ302から得たキーファイルKFと、ブラウザ格データ312とを格納してセキュアコンテナ832を作成する。

共通データベース830は、複数のコンテンツプロバイダ301が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツIDを用いて、コンテンツファイルCFを一元的に管理する。

また、図138に示すように、EMDサービスセンタ302が作成したキーフ

ファイルKFを、ユーザホームネットワーク303、303aのSAM305₁、305₁₂などに送るようにしてもよい。このときも、SAM305₁、305₁₂などに提供されたコンテンツファイルCFを作成したコンテンツプロバイダ301に対応するEMDサービスセンタ302からSAM305₁、305₁₂などにキーファイルKFが送られる。

また、サービスプロバイダ310は、コンテンツファイルCFをユーザホームネットワーク303に配給する。プライスタグデータ312は、サービスプロバイダ310がユーザホームネットワーク303に配給してもよいし、EMDサービスセンタ302がユーザホームネットワーク303、303aに配給してもよい。

第7実施形態

図139は本発明の第7実施形態のEMDシステムを説明するための図である。

本実施形態のEMDシステムは、前述した図136に示すEMDシステムと比較すると、コンテンツプロバイダ301からEMDサービスセンタ302にコンテンツデータのマスターソースS111を送り、EMDサービスセンタ302においてコンテンツファイルCFを作成する点が異なり、それ以外の点は略同じである。

コンテンツプロバイダ301は、コンテンツデータのマスターソースS111を複数のEMDサービスセンタ302のうち自らが選択した（あるいは予め決められた）一のEMDサービスセンタ302に送り、EMDサービスセンタ302において、図5（A）に示すコンテンツファイルCFを作成する。

EMDサービスセンタ302は、作成したコンテンツファイルCFを対応するコンテンツプロバイダ301に送る。

また、コンテンツプロバイダ301は、上記一の対応するEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データKc、電

子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容）、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格SRPを送り、EMDサービスセンタ302において図5（B）に示すキーファイルKFを作成する。

EMDサービスセンタ302は、作成したキーファイルKFを、対応するコンテンツプロバイダ301に送る。

また、EMDサービスセンタ302は、CFデータベース802aにコンテンツファイルCFを格納し、KFデータベース153aにキーファイルKFを格納し、個々のコンテンツデータに割り当てられたコンテンツIDを用いてコンテンツファイルCFおよびキーファイルKFを一元的に管理する。このとき、コンテンツIDは、例えば、EMDサービスセンタ302によって作成され、共通データベース840に格納される全てのセキュアコンテナ831に対応するコンテンツデータを対象としてグローバルユニークに決定される。

次に、コンテンツプロバイダ301において、対応するEMDサービスセンタ302から受けたコンテンツファイルCFおよびキーファイルKFとを格納したセキュアコンテナ841が作成され、セキュアコンテナ841が共通データベース840に格納される。

共通データベース840において、複数のコンテンツプロバイダ301が提供したセキュアコンテナ841が、コンテンツIDを用いて一元的に管理される。

サービスプロバイダ310は、例えば、コンテンツIDを用いて共通データベース840をブランジング（検索）して、所望のセキュアコンテナ841を共通データベース840から受けて、セキュアコンテナ841に、コンテンツの販売価格を示すプライスタグデータ312などをさらに格納したセキュアコンテナ842を作成し、セキュアコンテナ842をユーザホームネットワーク303に配

給する。

ユーザホームネットワーク 303 では、オンラインの場合には CA モジュール 311 を介してセキュアコンテナ 842 が SAM 305₁ などに提供され、SAM 305₁ などにおいて、キーファイル KF に格納されたコンテンツ鍵データ Kc および権利書データ 106 などが配信用鍵データ KD₁ ~ KD_n などを用いて復号され、復号された権利書データ 106 に基づいて、コンテンツファイル CF に格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、SAM 305₁ などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ 308 が生成され、利用履歴データ 308 が EMD サービスセンタ 302 に送信される。

また、ユーザホームネットワーク 303 の SAM 305₂ から、ユーザホームネットワーク 303 a の SAM 305₁₂ にセキュアコンテナ 832 が配給された場合には、SAM 305₁₂ において SAM 305₂ と同様の処理が行われ、SAM 305₁₂ から EMD サービスセンタ 302 に利用履歴データ 308 が送信される。

なお、ユーザホームネットワーク 303、303 a におけるセキュアコンテナ 807 に対しての処理は、前述した第 1 実施形態および第 2 実施形態におけるユーザホームネットワーク 103、303 における処理と同じである。

また、図 139 に示す例では、コンテンツプロバイダ 301 から共通データベース 840、共通データベース 840 からサービスプロバイダ 310、並びにサービスプロバイダ 310 からユーザホームネットワーク 303 に、コンテンツファイル CF およびキーファイル KF を格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイル CF およびキーファイル KF を同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。

また、図 140 に示すように、コンテンツプロバイダ 301 から共通データベース 830 にコンテンツファイル CF を格納し、サービスプロバイダ 310 が共

証局 2 の公開鍵データ K_{R-CA} 、EMD サービスセンタ 102 の公開鍵データ $K_{Esc, P}$ 、 $SAM105_1$ の秘密鍵データ $K_{SAM1, S}$ 、公開鍵証明書データ CER_{SAM1} およびその署名データ $SIG_{22, Esc}$ 、復号・伸長モジュール 163 およびメディア SAM との間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。

なお、公開鍵証明書データ CER_{SAM1} は、 $SAM105_1$ を出荷後に登録する際に EMD サービスセンタ 102 から $SAM105_1$ に送信してもよい。

また、記憶部 192 には、 $SAM105_1$ の出荷時に、図 5 に示すコンテンツファイル CF およびキーファイル KF を読み込み形式を示すファイルリダが、EMD サービスセンタ 102 によって書き込まれる。

$SAM105_1$ では、コンテンツファイル CF およびキーファイル KF に格納されたデータを利用する際に、記憶部 192 に記憶されたファイルリダが用いられる。

ここで、ルート認証局 2 の公開鍵データ K_{R-CA} は、インターネットの電子商取引などでは一般的に使用されている RSA を使用し、データ長は例えば 1024 ビットである。公開鍵データ K_{R-CA} は、図 1 に示すルート認証局 2 によって発行される。

また、EMD サービスセンタ 102 の公開鍵データ $K_{Esc, P}$ は、短いデータ長で RSA と同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば 160 ビットである。但し、暗号化の強度を考慮すると、公開鍵データ $K_{Esc, P}$ は 192 ビット以上であることが望ましい。また、EMD サービスセンタ 102 は、ルート認証局 92 に公開鍵データ $K_{Esc, P}$ を登録する。

また、ルート認証局 92 は、公開鍵データ $K_{Esc, P}$ の公開鍵証明書データ CER_{Esc} を作成する。公開鍵データ $K_{Esc, P}$ を格納した公開鍵証明書データ CER_{Esc} は、好ましく、 $SAM105_1$ の出荷時に記憶部 192 に記憶される。この

場合に、公開鍵証明書データ CER_{RSC} は、ルート認証局 92 の秘密鍵データ $K_{ROOT,S}$ で署名されている。

EMDサービスセンタ 102 は、乱数を発生して $SAM105_1$ の秘密鍵データ $K_{SAM1,S}$ を生成し、これとペアとなる公開鍵データ $K_{SAM1,P}$ を生成する。

また、EMDサービスセンタ 102 は、ルート認証局 92 の認証をもらって、公開鍵データ $K_{SAM1,P}$ の公開鍵証明書データ CER_{SAM1} を発行し、これに自らの秘密鍵データ $K_{RSC,S}$ を用いて署名データを添付する。すなわち、EMDサービスセンタ 102 は、セカンド CA（認証局）として機能を果たす。

また、 $SAM105_1$ には、図 24 に示す EMD サービスセンタ 102 の SAM 管理部 149 により、EMD サービスセンタ 102 の管理下にある一意（ユニーク）な識別子 SAM_ID が割り当てられ、これが $SAM105_1$ の記憶部 192 に格納されると共に、図 24 に示す SAM データベース 149a にも格納され、EMD サービスセンタ 102 によって管理される。

また、 $SAM105_1$ は、出荷後、例えば、ユーザによって EMD サービスセンタ 102 と接続され、登録手続を行うと共に、EMD サービスセンタ 102 から記憶部 192 に配信用鍵データ $KD_1 \sim KD_3$ が転送される。

すなわち、 $SAM105_1$ を利用するユーザは、コンテンツをダウンロードする前に EMD サービスセンタ 102 に登録手続が必要である。この登録手続は、例えば、 $SAM105_1$ を搭載している機器（当該例では、ネットワーク機器 160₁）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。

$SAM105_1$ は、上述した登録手続を経た後でないと使用できない。

EMD サービスセンタ 102 は、 $SAM105_1$ のユーザによる登録手続に応じて、ユーザに固有の識別子 $USER_ID$ を発行し、例えば、図 24 に示す SAM データベース 149a において、 SAM_ID と $USER_ID$ との対応関係を管理し、課金時に利用する。

また、EMDサービスセンタ102は、SAM105₁のユーザに対して情報参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子IDとパスワードとを用いて、EMDサービスセンタ102に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。

また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

次に、図30に示すように、SAM105₁内の記憶部192にSAM登録リストを格納する手順について説明する。

図1に示すSAM105₁は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり、新しい機器をバス191に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するSAM105₂～SAM105₄のSAM登録リストを得る。

なお、IEEE1394シリアルバスであるバス191に応じて生成されたトポロジーマップは、例えば、図44に示すように、バス191にSAM105₁～105₄に加えてAV機器160₁、160₂のSCMS処理回路105₁、105₂が接続されている場合に、SAM105₁～105₄およびSCMS処理回路105₁、105₂を対象として生成される。

従って、SAM105₁は、当該トポロジーマップから、SAM105₁～105₄についての情報を抽出して図45に示すSAM登録リストを生成する。

そして、SAM105₁は、図45に示すSAM登録リストを、EMDサービスセンタ102に登録して署名を得る。

これらの処理は、バス191のセッションを利用してSAM105₁が自動的にに行い、EMDサービスセンタ102にSAM登録リストの登録命令を発行する。

EMDサービスセンタ102は、SAM105₁から図45に示すSAM登録リストを受けると、有効期限を確認する。そして、EMDサービスセンタ102は、登録時にSAM105₁より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMDサービスセンタ102は、リボケーションリストをチェックしてSAM登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ102によって使用が禁止されている（無効な）SAMのリストである。

また、EMDサービスセンタ102は、決済時にはSAM105₁に対応するSAM登録リストを取り出し、その中に記述されたSAMがリボケーションリストに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。

これにより、図46に示すSAM登録リストが作成される。

なお、SAMリボケーションリストは、同一系の（同一のパス191に接続されている）SAMのみを対象として生成され、各SAMに対応するリボケーションフラグによって、当該SAMの有効および無効を示している。

以下、図1に示すコンテンツプロバイダ101の全体動作について説明する。

図47は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1：EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データK_{CP}の公開鍵証明書CER_{CP}をコンテンツプロバイダ101に送信する。

また、EMDサービスセンタ102は、SAM105₁～105₄が所定の登録処理を経た後に、SAM105₁～105₄の公開鍵データK_{SAM1-P}～K_{SAM4-P}の公開鍵証明書CER_{CP1}～CER_{CP4}をSAM105₁～105₄に送信する。

また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限

が1カ月の3カ月分の配信用鍵データKD₁～KD₃をユーザホームネットワーク103のSAM105₁～105₄に送信する。

このように、EMDシステム100では、配信用鍵データKD₁～KD₃を予めSAM105₁～105₄に配給しているため、SAM105₁～105₄とEMDサービスセンタ102との間がオフラインの状態でも、SAM105₁～105₄においてコンテンツプロバイダ101から配給されたセキュアコンテンツ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、SAM105₁～105₄とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーショニリストで無効の対象とする。

なお、利用制御状態データ166は、原則として、リアルタイムで、SAM105₁～105₄からEMDサービスセンタ102に送信される。

ステップS2:コンテンツプロバイダ101は、相互認証を行った後に、図18に示す登録用モジュールMod₂を、EMDサービスセンタ102に送信する。

そして、EMDサービスセンタ102は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データKcを登録して権威化する。

また、EMDサービスセンタ102は、登録用モジュールMod₂に応じた6カ月分のキーファイルKFを作成し、これをコンテンツプロバイダ101に送信する。

ステップS3:コンテンツプロバイダ101は、図5(A)、(B)に示すコンテンツファイルCFおよびその署名データSIG_{1.cr}と、キーファイルKFおよびその署名データSIG_{1.cr}とを作成し、これらと図5(C)に示す公開鍵証

明書データCER_oおよびその署名データSIG_{1, asc}とを格納したセキュアコンテナ104を、オンラインおよび／またはオフラインで、ユーザホームネットワーク103のSAM105₁～105₄に配給する。

オンラインの場合には、コンテンツプロバイダ用配送プロトコルを用いられ、当該プロトコルに依存しない形式で（すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして）、セキュアコンテナ104がコンテンツプロバイダ101からユーザホームネットワーク103に配送される。また、オフラインの場合には、ROM型あるいはRAM型の記録媒体に記録された状態で、セキュアコンテナ104が、コンテンツプロバイダ101からユーザホームネットワーク103に配送される。

ステップS4：ユーザホームネットワーク103のSAM105₁～SAM105₄は、コンテンツプロバイダ101から配給を受けたセキュアコンテナ104内の署名データSIG_{e, cp}、SIG_{τ, cp}、SIG_{x1, asc}を検証して、コンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認した後に、対応する期間の配信用鍵データKD₁～KD₄を用いてキーファイルKFを復号する。

ステップS5：SAM105₁～SAM105₄において、ユーザによる図25に示す購入・利用形態決定操作部165の操作に応じた操作信号S165に基づいて、購入・利用形態を決定する。

このとき、図31に示す利用監視部186において、セキュアコンテナ104に格納された権利書データ106に基づいて、ユーザによるコンテンツファイルCFの購入・利用形態が管理される。

ステップS6：SAM105₁～SAM105₄の図31に示す課金処理部187において、操作信号S165に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ108および利用制御状態データ166が生成し、これらをEMDサービスセンタ102に送信する。

ステップS7: EMDサービスセンタ102は、図24に示す決算処理部142において、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG_{ss}を、図1に示すペイメントゲートウェイ90を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

ステップS8: 決済機関91において、署名データSIG_{ss}の検証を行った後に、決済請求権データ152に基づいて、ユーザが支払った金額が、コンテンツプロバイダ101の所有者に分配される。

以上説明したように、EMDシステム100では、図5に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ101からユーザホームネットワーク103に配給し、セキュアコンテナ104内のキーファイルKFについての処理をSAM105₁～105₄内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁～KD₄を用いて暗号化されており、配信鍵データKD₁～KD₄を保持しているSAM105₁～105₄内でのみ復号される。そして、SAM105₁～105₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

従って、EMDシステム100によれば、ユーザホームネットワーク103におけるコンテンツデータCの購入および利用を、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。

また、EMDシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオ

フラインの何れの場合でもセキュアコンテナ104を用いて行うことで、SAM105₁～105₄におけるコンテンツデータCの権利処理を双方の場合において共通化できる。

また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂～160₄においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

図48は、第1実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。

図48に示すように、マルチプロセッサシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を配送するプロトコルとして例えばTCP/IPおよびXML/SMILが用いられる。

また、ユーザホームネットワーク103のSAM相互間でセキュアコンテナを転送するプロトコル、並びにユーザホームネットワーク103と103aとの間でセキュアコンテナを転送するプロトコルとして例えば1394シリアルバス・インタフェース上に構築されたXML/SMILが用いられる。また、この場合に、ROM型やRAM型の記録媒体にセキュアコンテナを記録してSAM相互間で配送してもよい。

第1実施形態の第1変形例

上述した実施形態では、図5(B)に示すように、EMDサービスセンタ102において配信用鍵データKDを用いてキーファイルKFを暗号化し、SAM105₁～105₄において配信用鍵データKDを用いてキーファイルKFを復号する場合を例示したが、図1に示すように、コンテンツプロバイダ101からSAM105₁～105₄にセキュアコンテナ104を直接供給する場合には、配信用鍵データKDを用いたキーファイルKFの暗号化は必ずしも行わなくても

よい。

このように、配信用鍵データKDを用いてキーファイルKFを暗号化することは、後述する第2実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データKDをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。

但し、上述した第1実施形態の場合でも、配信用鍵データKDを用いてキーファイルKFを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

また、上述した実施形態では、図5(B)に示すキーファイルKF内の権利書データ106内に標準小売価格データSRPを格納する場合を例示したが、セキュアコンテナ104内のキーファイルKFの外に、標準小売価格データSRP(プライスタグデータ)を格納してもよい。この場合には、標準小売価格データSRPに対して秘密鍵データK₀を用いて作成した署名データを添付する。

第1実施形態の第2変形例

上述した第1実施形態では、図1に示すように、EMDサービスセンタ102が、自らが生成した決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91で決済処理を行なう場合を例示したが、例えば、図49に示すように、EMDサービスセンタ102からコンテンツプロバイダ101に決済請求権データ152を送信し、コンテンツプロバイダ101自らが、決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91に対して決済処理を行なってもよい。

第1実施形態の第3変形例

上述した第1実施形態では、単数のコンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105_nに、セキュアコンテナ10

4を供給する場合を例示したが、2以上のコンテンツプロバイダ101a, 101bからSAM105₁～105₄にそれぞれセキュアコンテナ104a, 104bを供給するようにしてもよい。

図50は、コンテンツプロバイダ101a, 101bを用いる場合の第1実施形態の第3変形例に係わるEMDシステムの構成図である。

この場合には、EMDサービスセンタ102は、コンテンツプロバイダ101aおよび101bに、それぞれの6カ月分の配信用鍵データKD_{a1}～KD_a, およびKD_{b1}～KD_bを用いて暗号化したキーファイルKF_{a1}～KF_a, およびKF_{b1}～KF_bを配信する。

また、EMDサービスセンタ102は、SAM105₁～105₄に、3カ月分の配信用鍵データKD_{a1}～KD_a, およびKD_{b1}～KD_bを配信する。

そして、コンテンツプロバイダ101aは、独自のコンテンツ鍵データK_{c a}を用いて暗号化したコンテンツファイルCF_aと、EMDサービスセンタ102から受信した対応する期間のキーファイルKF_{a1}～KF_aとを格納したセキュアコンテナ104aをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。

このとき、キーファイルの識別子として、EMDサービスセンタ102が配付するグローバルユニークな識別子コンテンツIDが用いられ、EMDサービスセンタ102によって、コンテンツデータが一元的に管理される。

また、コンテンツプロバイダ101bは、独自のコンテンツ鍵データK_{c b}を用いて暗号化したコンテンツファイルCF_bと、EMDサービスセンタ102から受信した対応する期間のキーファイルKF_{b1}～KF_bとを格納したセキュアコンテナ104bをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。

SAM105₁～105₄は、セキュアコンテナ104aについては、対応す

る期間の配信用鍵データKD_{a1}～KD_{a3}を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108aおよび利用制御状態データ166aをEMDサービスセンタ102に送信する。

また、SAM105₁～105₄は、セキュアコンテナ104bについては、対応する期間の配信用鍵データKD_{b1}～KD_{b3}を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108bおよび利用制御状態データ166bをEMDサービスセンタ102に送信する。

EMDサービスセンタ102では、利用履歴データ108aに基づいて、コンテンツプロバイダ101aについての決済請求権データ152aを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102では、利用履歴データ108bに基づいて、コンテンツプロバイダ101bについての決済請求権データ152bを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102は、権利書データ106a、106bを登録して権威化を行なう。このとき、EMDサービスセンタ102は、権利書データ106a、106bに対応するキーファイルKF_a、KF_bに対して、グローバルユニークな識別子コンテンツIDを配付する。

また、EMDサービスセンタ102は、コンテンツプロバイダ101a、101bの公開鍵証明書データCER_{cpa}、CER_{cpb}を発行し、これに自らの署名データSIG_{1a,ESC}、SIG_{1b,ESC}を付してその正当性を認証する。

第1実施形態の第4変形例

上述した実施形態では、コンテンツファイルCFおよびキーファイルKFをディレクトリ構造でセキュアコンテナ104内に格納してコンテンツプロバイダ101からSAM105₁～105₄に送信する場合を例示したが、コンテンツフ

ファイルCFおよびキーファイルKFを、別々にSAM105₁～105₄に送信してもよい。

これには、例えば、以下に示す第1の手法と第2の手法とがある。

第1の手法では、図51に示すように、コンテンツプロバイダ101からSAM105₁～105₄に、通信プロトコルに依存しない形式で、コンテンツファイルCFおよびキーファイルKFを別々に送信する。

また、第2の手法では、図52に示すように、コンテンツプロバイダ101からSAM105₁～105₄にコンテンツファイルCFを通信プロトコルに依存しない形式で送信すると共に、EMDサービスセンタ102からSAM105₁～105₄にキーファイルKFを送信する。当該キーファイルKFの送信は、例えば、SAM105₁～105₄のユーザが、コンテンツデータCの購入形態を決定しようとするときに、EMDサービスセンタ102からSAM105₁～105₄に送信される。

上述した第1の手法および第2の手法を採用する場合には、関連するコンテンツファイルCF相互間と、コンテンツファイルCFとそれに対応するキーファイルKFとの間を、コンテンツファイルCFおよびキーファイルKFの少なくとも一方のヘッダに格納されたハイパーリンクデータを用いてリンク関係を確立する。SAM105₁～105₄では、当該リンク関係に基づいて、コンテンツデータCの権利処理および利用を行う。

なお、本変形例において、コンテンツファイルCFおよびキーファイルKFのフォーマットは、例えば、図5(A)、(B)に示すものが採用される。また、この場合に、コンテンツファイルCFおよびキーファイルKFと共に、それらの署名データSIG_{s, cp}、SIG_{t, cp}を送信することが好ましい。

第1実施形態の第5変形例

上述した実施形態では、セキュアコンテナ104内において、コンテンツファイルCFおよびキーファイルKFを別々に設けた場合を例示したが、例えば、図

53に示すように、セキュアコンテナ104内において、コンテンツファイルCF内にキーファイルKFを格納するようにしてもよい。

この場合に、キーファイルKFを格納したコンテンツファイルCFに対して、コンテンツプロバイダ101の秘密鍵データ K_{cp} による署名データが付される。

。

第1実施形態の第6変形例

上述した実施形態では、コンテンツデータCをコンテンツファイルCFに格納し、コンテンツ鍵データKcおよび権利書データ106をキーファイルKF内に格納してコンテンツプロバイダ101からSAM105₁などに送信する場合を例示したが、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106の少なくとも一つをファイル形式を採用せずにコンテンツプロバイダ101からSAM105₁などに、通信プロトコルに依存しない形式で送信してもよい。

例えば、図54に示すように、コンテンツプロバイダ101において、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFとを格納したセキュアコンテナ104sを作成し、セキュアコンテナ104sをSAM105₁などに通信プロトコルに依存しない形式で送信してもよい。

また、図55に示すように、コンテンツプロバイダ101からSAM105₁などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFとを通信プロトコルに依存しない形式で個別に送信してもよい。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと同一経路で送信する。

また、図56に示すように、コンテンツプロバイダ101からSAM105₁

などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCを通信プロトコルに依存しない形式で送信すると共に、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFをEMDサービスセンタ102からSAM105₁などに送信してもよい。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと別経路で送信する。

また、図57に示すように、コンテンツプロバイダ101からSAM105₁などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106とを、通信プロトコルに依存しない形式で送信してもよい。すなわち、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106をファイル形式にしないで、同一経路で送信する。

また、図58に示すように、コンテンツプロバイダ101からSAM105₁などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCを、通信プロトコルに依存しない形式で送信すると共に、EMDサービスセンタ102からSAM105₁などにコンテンツ鍵データKcおよび権利書データ106を送信してもよい。すなわち、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106をファイル形式にしないで、別経路で送信する。

第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配給する場合について説明する。

図59は、本実施形態のEMDシステム300の構成図である。

図59に示すように、EMDシステム300は、コンテンツプロバイダ301

、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。

コンテンツプロバイダ301、EMDサービスセンタ302、SAM305₁～305₄。およびサービスプロバイダ310は、それぞれ請求項22および請求項152などに係るデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。

また、EMDサービスセンタ302は、コンテンツプロバイダ101およびSAM505₁～505₄に加えて、サービスプロバイダ310に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。

また、ユーザホームネットワーク303は、ネットワーク機器360₁およびAV機器360₂～360₄を有している。ネットワーク機器360₁はSAM305₁およびCAMジュール311を内蔵しており、AV機器360₂～360₄はそれぞれSAM305₂～305₄を内蔵している。

ここで、SAM305₁～305₄は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）309の作成を行なう点とを除いて、前述した第1実施形態のSAM105₁～105₄と同じである。

先ず、EMDシステム300の概要について説明する。

EMDシステム300では、コンテンツプロバイダ301は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書(UCP:Usage Control Policy)データ106

およびコンテンツ鍵データKcを、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106およびコンテンツ鍵データKcは、EMDサービスセンタ302に登録されて権威化（認証）される。

また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から、各コンテンツファイルCFについて、それぞれ6か月分のキーファイルKFを受信する。

当該キーファイルKF内には、当該キーファイルKFの改竄の有無、当該キーファイルKFの作成者および送信者の正当性を検証するための署名データが格納されている。

そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納した図5に示すセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどでサービスプロバイダ310に供給する。

また、セキュアコンテナ104に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104の作成者および送信者の確認する。

次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対しての価格（SRP）に、自らが行ったオーサリングなどのサービスに対しての価格を加算した価格を示すプライスタグデータ（PT）312を作成する。

そして、サービスプロバイダ310は、セキュアコンテナ104から取り出し

たコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ312と、これらに対しての自らの秘密鍵データ K_{sp} による署名データとを格納したセキュアコンテナ304を作成する。

このとき、キーファイルKFは、配信用鍵データ $KD_1 \sim KD_n$ によって暗号化されており、サービスプロバイダ310は当該配信用鍵データ $KD_1 \sim KD_n$ を保持していないため、サービスプロバイダ310はキーファイルKFの中身を見たり、書き換えたりすることはできない。

また、EMDサービスセンタ302は、プライスタグデータ312を登録して権威化する。

サービスプロバイダ310は、オンラインおよび／またはオフラインでセキュアコンテナ304をユーザホームネットワーク303に配給する。

このとき、オフラインの場合には、セキュアコンテナ304はROM型の記録媒体などに記録されてSAM305₁～305_nにそのまま供給される。一方、オンラインの場合には、サービスプロバイダ310とCAモジュール311との間で相互認証を行い、セキュアコンテナ304をサービスプロバイダ310においてセッション鍵データ K_{ss} を用いた暗号化して送信し、CAモジュール311において受信したセキュアコンテナ304をセッション鍵データ K_{ss} を用いて復号した後に、SAM305₁～305_nに転送する。

この場合に、コンテンツプロバイダ301からユーザホームネットワーク303にセキュアコンテナ304を送信する通信プロトコルとして、デジタル放送であればMHEG(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットであればXML/SMIL/HTML(Hyper TextMarkup Language)が用いられ、これらの通信プロトコル内に、セキュアコンテナ304が、当該通信プロトコル(符号化方式など)に依存しない形式でトンネリングして埋め込まれる。

従って、通信プロトコルとセキュアコンテナ304との間でフォーマットの整

合性をとる必要性はなく、セキュアコンテナ304のフォーマットを柔軟に設定できる。

次に、SAM305₁～305₄において、セキュアコンテナ304内に格納された署名データを検証して、セキュアコンテナ304に格納されたコンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認する。そして、SAM305₁～305₄において、当該正当性が確認されると、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD₁～KD₄を用いてキーファイルKFを復号する。

SAM305₁～305₄に供給されたセキュアコンテナ304は、ネットワーク機器360₁およびAV機器360₂～360₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM305₁～305₄は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴(Usage Log)データ308として記録する。

利用履歴データ(履歴データまたは管理装置用履歴データ)308は、例えば、EMDサービスセンタ302からの要求に応じて、ユーザホームネットワーク303からEMDサービスセンタ302に送信される。

また、SAM305₁～305₄は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御状態データ(UCS:Usage control state Data)166をEMDサービスセンタ302に送信する。

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分

配される。

本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、EMDサービスセンタ302は、中立の立場にある最高の権威機関であるルート認証局92に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ301の権利書データ106、コンテンツ鍵データKcおよびサービスプロバイダ310のプライスタグデータ312を登録して権威化することも、EMDサービスセンタ302の認証機能によるものである。

また、EMDサービスセンタ302は、例えば、配信用鍵データKD₁～KD_nなどの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301が登録した権利書データ106とSAM305₁～SAM305₄から入力した利用履歴データ308とサービスプロバイダ310が登録したプライスタグデータ312とに基づいて、ユーザホームネットワーク303のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ301およびサービスプロバイダ310に分配して支払う権利処理（利益分配）機能を有する。

以下、コンテンツプロバイダ301の各構成要素について詳細に説明する。

〔コンテンツプロバイダ301〕

図60は、コンテンツプロバイダ301の機能ブロック図であり、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されて

いる。

図 60 に示すように、コンテンツプロバイダ 301 は、コンテンツマスターデータベース 111、電子透かし情報付加部 112、圧縮部 113、暗号化部 114、乱数発生部 115、署名処理部 117、セキュアコンテナ作成部 118、セキュアコンテナデータベース 118a、キーファイルデータベース 118b、記憶部 119、相互認証部 120、暗号化・復号部 121、権利書データ作成部 122、EMD サービスセンタ管理部 125 および サービスプロバイダ管理部 324 を有する。

図 60 において、図 3 と同一符号を付した構成要素は、前述した第 1 実施形態において図 3 および図 4 を参照しながら説明した同一符号の構成要素と同じである。

すなわち、コンテンツプロバイダ 301 は、図 3 に示す SAM 管理部 124 の代わりに サービスプロバイダ管理部 324 を設けた構成をしている。

サービスプロバイダ管理部 324 は、セキュアコンテナ作成部 118 から入力した図 5 に示すセキュアコンテナ 104 を、オフラインおよび／またはオンラインで、図 59 に示す サービスプロバイダ 310 に提供する。

サービスプロバイダ管理部 324 は、図 5 に示すセキュアコンテナ 104 をオンラインで サービスプロバイダ 310 に配信する場合には、暗号化・復号部 121 においてセッション鍵データ K_{ss} を用いてセキュアコンテナ 104 を暗号化した後に、ネットワークを介して サービスプロバイダ 310 に配信する。

また、図 4 に示すコンテンツプロバイダ 101 内でのデータの流れは、コンテンツプロバイダ 301 にも同様に適用される。

以下、コンテンツプロバイダ 301 から サービスプロバイダ 310 にセキュアコンテナ 104 を送信する際の処理の流れを説明する。

図 61 および図 62 は、コンテンツプロバイダ 301 から サービスプロバイダ 310 にセキュアコンテナ 104 を送信する際の処理の流れを示すフローチャー

トである。

ステップC1: コンテンツプロバイダ301とサービスプロバイダ310との間で相互認証を行う。

ステップC2: ステップC1の相互認証によって得られたセッション鍵データ K_{ss} を、コンテンツプロバイダ301およびサービスプロバイダ310の間で共有する。

ステップC3: サービスプロバイダ310によって、コンテンツプロバイダ301が所有する(CP用)セキュアコンテナデータベース118aにアクセスが行われる。

ステップC4: サービスプロバイダ310は、例えば、セキュアコンテナデータベース118aにおいて一元的に管理されているコンテンツIDとメタデータとのリストを参照して自らの配信サービスに必要なセキュアコンテナ104を選択する。

ステップC5: コンテンツプロバイダ301は、ステップC4で選択したセキュアコンテナ104を、ステップC2で共有したセッション鍵データ K_{ss} を用いて暗号化する。

ステップC6: コンテンツプロバイダ301は、ステップC5で得られたセキュアコンテナ104を、コンテンツプロバイダ用商品配送プロトコルに挿入する。

ステップC7: サービスプロバイダ310は、ダウンロードを行う。

ステップC8: サービスプロバイダ310は、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテナ104を取り出す。

ステップC9: サービスプロバイダ310は、セキュアコンテナ104を、ステップC2で共有したセッション鍵データ K_{ss} を用いて復号する。

ステップC10: サービスプロバイダ310は、復号したセキュアコンテナ104に格納されている署名データを検証して、送信者の正当性を確認し、送信者

が正当であることの確認を条件にステップC11の処理を行う。

ステップC11：サービスプロバイダ310は、セキュアコンテナ104を自らのセキュアコンテナデータベースに格納する。

〔サービスプロバイダ310〕

サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したプライスタグデータ312とを格納したセキュアコンテナ304を作成し、ユーザホームネットワーク303のネットワーク機器360₁およびAV機器360₂～360₄にセキュアコンテナ304をオンラインおよび／またはオフラインで配給する。

サービスプロバイダ310によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

図63は、サービスプロバイダ310の機能ブロック図である。

なお、図63には、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104を用いて作成したセキュアコンテナ304をユーザホームネットワーク303に供給する際のデータの流れが示されている。

図63に示すように、サービスプロバイダ310は、コンテンツプロバイダ管理部350、記憶部351、相互認証部352、暗号化・復号部353、署名処理部354、セキュアコンテナ作成部355、セキュアコンテナデータベース355a、プライスタグデータ作成部356、ユーザホームネットワーク管理部3

57、EMDサービスセンタ管理部358およびユーザ嗜好フィルタ生成部920を有する。

以下、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104からセキュアコンテナ304を作成し、これをユーザホームネットワーク303に配給する際のサービスプロバイダ310内での処理の流れを図63および図64を参照しながら説明する。

図64は、コンテンツプロバイダ301からユーザホームネットワーク303にセキュアコンテナ304を配給する処理を説明するためのフローチャートである。

<ステップD1>

コンテンツプロバイダ管理部350は、オンラインおよび／またはオフラインで、コンテンツプロバイダ301から図5に示すセキュアコンテナ104の供給を受けてセキュアコンテナ104を記憶部351に書き込む。

このとき、コンテンツプロバイダ管理部350は、オンラインの場合には、図60に示す相互認証部120と図63に示す相互認証部352との間の相互認証によって得られたセッション鍵データ K_{ss} を用いて、セキュアコンテナ104を暗号化・復号部353において復号した後に、記憶部351に書き込む。

なお、サービスプロバイダ310は、記憶部351とは別に、セキュアコンテナ104を格納するための専用のセキュアコンテナデータベースを有してもよい。

<ステップD2>

次に、署名処理部354において、記憶部351に記憶されているセキュアコンテナ104の図5(C)に示す署名データ $SIG_{1,ssc}$ を、記憶部351から読み出したEMDサービスセンタ302の公開鍵データ $K_{ssc,p}$ を用いて検証し、その正当性が認められた後に、図5(C)に示す公開鍵証明書データ CER_{cp} から公開鍵データ K_{cp} を取り出す。

次に、署名処理部354は、当該取り出した公開鍵データ $K_{cp,r}$ を用いて、記憶部351に記憶されているセキュアコンテナ104の図5(A), (B)に示す署名データ $SIG_{s,cp}$, $SIG_{7,cp}$ の検証、すなわちコンテンツファイルCFの作成者および送信者と、キーファイルKFの送信者との正当性の検証を行う。

また、署名処理部354は、記憶部351から読み出した公開鍵データ $K_{k1,esc}$ を用いて、図5(B)に示すキーファイルKFに格納された署名データ $SIG_{k1,esc}$ の検証、すなわちキーファイルKFの作成者の正当性の検証を行う。このとき、署名データ $SIG_{k1,esc}$ の検証は、キーファイルKFがEMDサービスセンタ302に登録されているか否かの検証も兼ねている。

<ステップD3>

次に、セキュアコンテナ作成部355は、署名データ $SIG_{s,cp}$, $SIG_{7,cp}$, $SIG_{k1,esc}$ の正当性が確認されると、記憶部351からコンテンツファイルCFおよびその署名データ $SIG_{s,cp}$ と、キーファイルKFおよびその署名データ $SIG_{7,cp}$ と、サービスプロバイダ310の公開鍵証明書データ CER_{sp} およびその署名データ $SIG_{s1,esc}$ と、コンテンツプロバイダ301の公開鍵証明書データ CER_{cp} およびその署名データ $SIG_{1,esc}$ とを読み出す。

また、プライスタグデータ作成部356は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ312を作成し、記憶部351に記憶する。

また、署名処理部354は、コンテンツファイルCF、キーファイルKFおよびプライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データ $K_{sp,r}$ を用いて、署名データ $SIG_{s2,sp}$, $SIG_{s3,sp}$, $SIG_{s4,sp}$ を作成し、これをセキュアコンテナ作成部355に出力する。

ここで、署名データ $SIG_{s2,sp}$ はコンテンツファイルCFの送信者の正当性

を検証するために用いられ、署名データSIG_{ss, sp}はキーファイルKFの送信者の正当性を検証するために用いられ、署名データSIG_{sa, sp}はプライスタグデータ312の作成者および送信者の正当性を検証するために用いられる。

次に、セキュアコンテナ作成部355は、図65(A)～(D)に示すように、コンテンツファイルCFおよびその署名データSIG_{sc, cp}、SIG_{ss, sp}と、キーファイルKFおよびその署名データSIG_{sc, cp}、SIG_{ss, sp}と、プライスタグデータ312およびその署名データSIG_{sa, sp}と、公開鍵証明書データCER_{sp}およびその署名データSIG_{sl, sp}と、公開鍵証明書データCER_{cp}およびその署名データSIG_{sl, sp}とを格納したセキュアコンテナ304を作成し、セキュアコンテナデータベース355aに格納する。

セキュアコンテナデータベース355aに格納されたセキュアコンテナ304は、例えば、コンテンツIDなどを用いてサービスプロバイダ310によって一元的に管理される。

<ステップD4>

セキュアコンテナ作成部355は、ユーザホームネットワーク303からの要求に応じたセキュアコンテナ304をセキュアコンテナデータベース355aから読み出してユーザホームネットワーク管理部357に出力する。

このとき、セキュアコンテナ304は、複数のコンテンツファイルCFと、それらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルCFを単数のセキュアコンテナ304に格納してもよい。これらの複数のコンテンツファイルCFなどは、ディレクトリー構造でセキュアコンテナ304内に格納してもよい。

また、セキュアコンテナ304は、デジタル放送で送信される場合には、MH EG(Multimedia and Hypermedia information coding Experts Group)プロトコ

ルが用いられ、インターネットで送信される場合にはXML/SMIL/HTML(Hyper TextMarkup Language) プロトコルが用いられる。

このとき、セキュアコンテナ304内のコンテンツファイルCFおよびキーファイルKFなどは、MHEGおよびHTMLのプロトコルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ310とユーザホームネットワーク303との間で採用される通信プロトコル内の所定の階層に格納される。

例えば、セキュアコンテナ304をデジタル放送で送信する場合には、図66に示すように、コンテンツファイルCFが、MHEGオブジェクト(Object)内のMHEGコンテンツデータとして格納される。

また、MHEGオブジェクトは、トランスポート層プロトコルにおいて、動画である場合にはPES(Packetized Elementary Stream)-Videoに格納され、音声である場合にはPES-Audioに格納され、静止画である場合にはPrivate-Dataに格納される。

また、図67に示すように、キーファイルKF、プライスタグデータ312および公開鍵証明書データCER_{cr}、CER_{sr}は、トランスポート層プロトコルのTS Packet 内のECM(Entitlement Control Message) に格納される。

ここで、コンテンツファイルCF、キーファイルKF、プライスタグデータ312および公開鍵証明書データCER_{cr}、CER_{sr}は、コンテンツファイルCFのヘッダ内のディレクトリ構造データDSD₁によって相互間のリンクが確立されている。

次に、ユーザホームネットワーク管理部357は、セキュアコンテナ304を、オフラインおよび/またはオンラインでユーザホームネットワーク303に供給する。

ユーザホームネットワーク管理部357は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器360₁に配信する

場合には、相互認証後に、暗号化・復号部 352 においてセッション鍵データ K_{ss} を用いてセキュアコンテナ 304 を暗号化した後に、ネットワークを介してネットワーク機器 360₁ に配信する。

なお、ユーザホームネットワーク管理部 357 は、セキュアコンテナ 304 を例えば衛星などを介して放送する場合には、セキュアコンテナ 304 をスクランブル鍵データ K_{scr} を用いて暗号化する。また、スクランブル鍵データ K_{scr} をワーク鍵データ K_w を暗号化し、ワーク鍵データ K_w をマスタ鍵データ K_M を用いて暗号化する。

そして、ユーザホームネットワーク管理部 357 は、セキュアコンテナ 304 と共に、スクランブル鍵データ K_{scr} およびワーク鍵データ K_w を、衛星を介してユーザホームネットワーク 303 に送信する。

また、例えば、マスタ鍵データ K_M を、ICカードなどに記憶してオフラインでユーザホームネットワーク 303 に配給する。

また、ユーザホームネットワーク管理部 357 は、ユーザホームネットワーク 303 から、当該サービスプロバイダ 310 が配給したコンテンツデータ C に関する SP 用購入履歴データ 309 を受信すると、これを記憶部 351 に書き込む。

サービスプロバイダ 310 は、将来のサービス内容を決定する際に、SP 用購入履歴データ 309 を参照する。また、ユーザ嗜好フィルタ生成部 920 は、SP 用購入履歴データ 309 に基づいて、当該 SP 用購入履歴データ 309 を送信した SAM 305₁ ~ 305₄ のユーザの嗜好を分析してユーザ嗜好フィルタデータ 900 を生成し、これをユーザホームネットワーク管理部 357 を介してユーザホームネットワーク 303 の CA モジュール 311 に送信する。

図 68 には、サービスプロバイダ 310 内における EMD サービスセンタ 302 との間の通信に関連するデータの流れが示されている。

なお、以下に示す処理を行う前提として、サービスプロバイダ 310 の関係者

は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ302に登録処理を行い、グローバルユニークな識別子SP_IDを得ている。識別子SP_IDは、記憶部351に記憶される。

先ず、サービスプロバイダ310が、EMDサービスセンタ302に、自らの秘密鍵データ $K_{sp,s}$ に対応する公開鍵データ $K_{sp,p}$ の正当性を証明する公開鍵証明書データ CER_{sp} を要求する場合の処理を図68を参照しながら説明する。

サービスプロバイダ310は、真性乱数発生器を用いて乱数を発生して秘密鍵データ $K_{sp,s}$ を生成し、当該秘密鍵データ $K_{sp,s}$ に対応する公開鍵データ $K_{sp,p}$ を作成して記憶部351に記憶する。

EMDサービスセンタ管理部358、サービスプロバイダ310の識別子SP_IDおよび公開鍵データ $K_{sp,p}$ を記憶部351から読み出す。

そして、EMDサービスセンタ管理部358は、識別子SP_IDおよび公開鍵データ $K_{sp,p}$ を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ管理部348は、当該登録に応じて、公開鍵証明書データ CER_{sp} およびその署名データ $SIG_{s1,ssc}$ をEMDサービスセンタ302から入力して記憶部351に書き込む。

次に、サービスプロバイダ310が、EMDサービスセンタ302にプライスタグデータ312を登録して権威化する場合の処理を図68を参照して説明する。

この場合には、署名処理部354において、記憶部351から読み出したプライスタグデータ312およびグローバルユニークな識別子であるコンテンツIDを格納した図69に示すモジュール Mod_{102} のハッシュ値が求められ、秘密鍵データ $K_{sp,s}$ を用いて署名データ $SIG_{s1,ssc}$ が生成される。

また、記憶部351から公開鍵証明書データ CER_{sp} およびその署名データ $SIG_{s1,ssc}$ が読み出される。

そして、図 69 に示すプライスタグ登録要求用モジュール Mod_{102} が、相互認証部 352 と EMD サービスセンタ 302 との間の相互認証によって得られたセッション鍵データ K_{ss} を用いて暗号化・復号部 353 において暗号化された後に、EMD サービスセンタ管理部 358 から EMD サービスセンタ 302 に送信される。

なお、モジュール Mod_{102} に、サービスプロバイダ 310 のグローバルユニークな識別子 SP_ID を格納してもよい。

また、EMD サービスセンタ管理部 358 は、EMD サービスセンタ 302 から受信した決済レポートデータ 307s を記憶部 351 に書き込む。

また、EMD サービスセンタ管理部 358 は、EMD サービスセンタ 302 から受信したマーケティング情報データ 904 を記憶部 351 に記憶する。

マーケティング情報データ 904 は、サービスプロバイダ 310 が今後配給するコンテンツデータ C を決定する際に参考される。

(EMD サービスセンタ 302)

EMD サービスセンタ 302 は、前述したように、認証局 (CA: Certificate Authority)、鍵管理 (Key Management) 局および権利処理 (Rights Clearing) 局としての役割を果たす。

図 70 は、EMD サービスセンタ 302 の機能の構成図である。

図 70 に示すように、EMD サービスセンタ 302 は、鍵サーバ 141、鍵データベース 141a、KF 作成部 153、決済処理部 442、署名処理部 443、決算機関管理部 144、証明書・権利害管理部 445、権利害データベース 445a、証明書データベース 445b、コンテンツプロバイダ管理部 148、CP データベース 148a、SAM 管理部 149、SAM データベース 149a、相互認証部 150、暗号化・復号部 151、サービスプロバイダ管理部 390、SP データベース 390a、コンテンツ ID 作成部 851、ユーザ嗜好フィルタ生成部 901 およびマーケティング情報データ生成部 902 を有する。

図 70 において、図 23 および図 24 と同じ符号を付した機能ブロックは、第 1 実施形態で説明した同一符号の機能ブロックと略同じ機能を有している。

以下、図 70 において、新たな符号を付した機能ブロックについて説明する。

なお、図 70 には、EMD サービスセンタ 302 内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ 310 との間で送受信されるデータに関連するデータの流れが示されている。

また、図 71 には、EMD サービスセンタ 302 内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ 301 との間で送受信されるデータに関連するデータの流れが示されている。

また、図 72 には、EMD サービスセンタ 302 内の機能ブロック相互間のデータの流れのうち、図 59 に示す SAM305₁～305₄、および決済機関 91 との間で送受信されるデータに関連するデータの流れが示されている。

決済処理部 442 は、図 72 に示すように、SAM305₁～305₄ から入力した利用履歴データ 308 と、証明書・権利書管理部 445 から入力した標準小売価格データ SRP およびプライスタグデータ 312 に基づいて決済処理を行う。なお、この際に、決済処理部 442 は、サービスプロバイダ 310 によるダンピングの有無などを監視する。

決済処理部 442 は、決済処理により、図 72 に示すように、コンテンツプロバイダ 301 についての決済レポートデータ 307c および決済請求権データ 152c を作成し、これらをそれぞれコンテンツプロバイダ管理部 148 および決済機関管理部 144 に出力する。

また、決済処理により、図 70 および図 72 に示すように、サービスプロバイダ 310 についての決済レポートデータ 307s および決済請求権データ 152s を作成し、これらをそれぞれサービスプロバイダ管理部 390 および決済機関管理部 144 に出力する。

ここで、決済請求権データ152c, 152sは、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータである。

ここで、利用履歴データ308は、第1実施形態で説明した利用履歴データ108と同様に、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。利用履歴データ308には、例えば、図73に示すように、セキュアコンテナ304に格納されたコンテンツデータCの識別子であるコンテンツID、セキュアコンテナ304に格納されたコンテンツデータCを提供したコンテンツプロバイダ301の識別子CP_ID、セキュアコンテナ304を配給したサービスプロバイダ310の識別子SP_ID、コンテンツデータCの信号諸元データ、セキュアコンテナ304内のコンテンツデータCの圧縮方法、セキュアコンテナ304を記録した記録媒体の識別子Media_ID、セキュアコンテナ304を配給を受けたSAM305₁～305₄の識別子SAM_ID、当該SAM105₁～105₄のユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ302は、コンテンツプロバイダ301およびサービスプロバイダ310の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク303のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

証明書・権利書管理部445は、証明書データベース445bに登録されて権威化された公開鍵証明書データCER_{cp}、公開鍵証明書データCER_{sp}および公開鍵証明書データCER_{sam1}～CER_{sam2}などを読み出すと共に、権利書データベース445aにコンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データKc、並びにサービスプロバイダ310のプライスタグデータ312などを登録して権威化する。

このとき、証明書・権利書管理部445は、権利書データ106、コンテンツ

鍵データKcおよびプライスタグデータ312などのハッシュ値をとり、秘密鍵データK_{sec.}を用いた署名データを付して権威化証明書データを作成する。

コンテンツプロバイダ管理部148は、コンテンツプロバイダ101との間で通信する機能を有し、登録されているコンテンツプロバイダ101の識別子CP_IDなどを管理するCPデータベース148aにアクセスできる。

ユーザ嗜好フィルタ生成部901は、利用履歴データ308に基づいて、当該利用履歴データ308を送信したSAM305₁～305₄のユーザの嗜好に応じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ903を生成し、ユーザ嗜好フィルタデータ903をSAM管理部149を介して、当該利用履歴データ308を送信したSAM305₁～305₄に送信する。

マーケティング情報データ生成部902は、利用履歴データ308に基づいて、例えば、複数のサービスプロバイダ310によってユーザホームネットワーク103に配給されたコンテンツデータCの全体の購入状況などを示すマーケティング情報データ904を生成し、これをサービスプロバイダ管理部390を介して、サービスプロバイダ310に送信する。サービスプロバイダ310は、マーケティング情報データ904を参考にして、今後提供するサービスの内容を決定する。

以下、EMDサービスセンタ302内での処理の流れを説明する。

EMDサービスセンタ302からSAM305₁～305₄への配信用鍵データKD₁～KD₄の送信は、第1実施形態の場合と同様に行なわれる。

また、EMDサービスセンタ302がコンテンツプロバイダ301から、公開鍵証明書データの発行要求を受けた場合の処理は証明書・権利書管理部445が証明書データベース445bにアクセスする点を除いて、前述した第1実施形態と同じである。また、権利書データ106などを登録する処理も、証明書・権利書管理部445が権利書データベース445aに当該データを格納する点を除いて前述した第1実施形態の場合と同様である。

次に、EMDサービスセンタ302がサービスプロバイダ310から、公開鍵証明書データの発行要求を受けた場合の処理を、図70を参照しながら説明する。

この場合に、サービスプロバイダ管理部390は、予めEMDサービスセンタ302によって与えられたサービスプロバイダ310の識別子SP_ID、公開鍵データK_{sp}、および署名データSIG_{70,sp}をサービスプロバイダ310から受信すると、これらを、相互認証部150と図63に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{ss}を用いて復号する。

そして、当該復号した署名データSIG_{70,sp}の正当性を署名処理部443において確認した後に、識別子SP_IDおよび公開鍵データK_{sp}に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ310がSPデータベース390aに登録されているか否かを確認する。

そして、証明書・権利書管理部445は、当該サービスプロバイダ310の公開鍵証明書データCER_{sp}を証明書データベース445bから読み出してサービスプロバイダ管理部390に出力する。

また、署名処理部443は、公開鍵証明書データCER_{sp}のハッシュ値をとり、EMDサービスセンタ302の秘密鍵データK_{sec}を用いて、署名データSIG_{81,sec}を作成し、これをサービスプロバイダ管理部390に出力する。

そして、サービスプロバイダ管理部390は、公開鍵証明書データCER_{sp}およびその署名データSIG_{81,sec}を、相互認証部150と図63に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{ss}を用いて暗号化した後に、サービスプロバイダ310に送信する。

なお、EMDサービスセンタ302がSAM1051～1054から、公開鍵証明書データの発行要求を受けた場合の処理は、第1実施形態と同様である。

また、EMDサービスセンタ302が、コンテンツプロバイダ301から権利書データ106およびコンテンツ鍵データKcの登録要求を受けた場合の処理も

、第1実施形態と同様である。

また、EMDサービスセンタ302が、コンテンツプロバイダ301から受信した登録用モジュールMod₂に応じてキーファイルKFを作成してコンテンツプロバイダ301に送信する処理も、第1実施形態と同様である。

次に、EMDサービスセンタ302が、サービスプロバイダ310からブライスタグデータ312の登録要求を受けた場合の処理を、図70を参照しながら説明する。

この場合には、サービスプロバイダ管理部390がサービスプロバイダ310から図69に示すブライスタグ登録要求モジュールMod₁₀₂を受信すると、相互認証部150と図63に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{ss}を用いてブライスタグ登録要求モジュールMod₁₀₂を復号する。

そして、当該復号したブライスタグ登録要求モジュールMod₁₀₂に格納された署名データSIG_{00,sp}の正当性を署名処理部443において確認した後に、ブライスタグ登録要求モジュールMod₁₀₂に格納されたブライスタグデータ312を、証明書・権利書管理部445を介して権利書データベース445aに登録して権威化する。

次に、EMDサービスセンタ302において決済を行なう場合の処理を図72を参照しながら説明する。

SAM管理部149は、ユーザホームネットワーク303の例えばSAM305₁から利用履歴データ308およびその署名データSIG_{205,SAM1}を入力すると、利用履歴データ308および署名データSIG_{205,SAM1}を、相互認証部150とSAM305₁～305₄との間の相互認証によって得られたセッション鍵データK_{ss}を用いて復号し、SAM305₁の公開鍵データK_{SAM1,p}を用いて署名データSIG_{205,SAM1}の検証を行なった後に、決済処理部442に出力する。

。

そして、決済処理部442は、SAM305₁から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312とに基づいて決済処理を行う。

決済処理部442は、決済処理により、図72に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。

また、決済処理により、図70および図72に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。

次に、決算機関管理部144は、決済請求権データ152c、152sと、それらについて秘密鍵データK_{sec.}を用いて作成した署名データとを、相互認証およびセッション鍵データK_{ss.}による復号を行なった後に、図59に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152cに示される金額の金銭がコンテンツプロバイダ301に支払われ、決済請求権データ152sに示される金額の金銭がサービスプロバイダ310に支払われる。

次に、EMDサービスセンタ302がコンテンツプロバイダ301およびサービスプロバイダ310に決済レポートデータ307cおよび307sを送信する場合の処理を説明する。

決済処理部442において決済が行なわれると、決済処理部442からコンテンツプロバイダ管理部148に決済レポートデータ307cが出力される。

コンテンツプロバイダ管理部148は、決済処理部442から決済レポートデータ307cを入力すると、これを、相互認証部150と図60に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{ss.}を用いて暗号化し

た後に、コンテンツプロバイダ301に送信する。

また、決算処理部442において決済が行なわれると、決算処理部442からサービスプロバイダ管理部390に決済レポートデータ307sが出力される。

サービスプロバイダ管理部390は、決算処理部442から決済レポートデータ307sを入力すると、これを、相互認証部150と図63に示す相互認証部352との相互認証で得られたセッション鍵データ K_{ss} を用いて暗号化した後に、サービスプロバイダ310に送信する。

EMDサービスセンタ302は、その他に、第1実施形態のEMDサービスセンタ102と同様に、SAM305₁～305₄の出荷時の処理と、SAM登録リストの登録処理とを行なう。

〔ユーザホームネットワーク303〕

ユーザホームネットワーク303は、図59に示すように、ネットワーク機器360₁およびA/V機器360₂～360₄を有している。

ネットワーク機器360₁は、CAMモジュール311およびSAM305₁を内蔵している。また、AV機器360₂～360₄は、それぞれSAM305₂～305₄を内蔵している。

SAM305₁～305₄の相互間は、例えば、1394シリアルインタフェースバスなどのバス191を介して接続されている。

なお、AV機器360₂～360₄は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器360₁のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク303は、ネットワーク機能を有していないAV機器のみを有していてもよい。

以下、ネットワーク機器360₁について説明する。

図74は、ネットワーク機器360₁の構成図である。

図 74 に示すように、ネットワーク機器 360₁ は、通信モジュール 162、CAモジュール 311、復号モジュール 905、SAM305₁、復号・伸長モジュール 163、購入・利用形態決定操作部 165、ダウンロードメモリ 167、再生モジュール 169 および外部メモリ 201 を有する。

図 74 において、図 25 と同一符号を付した構成要素は、第 1 実施形態で説明した同一符号の構成要素と同じである。

通信モジュール 162 は、サービスプロバイダ 310 との間の通信処理を行なう。

具体的には、通信モジュール 162 は、サービスプロバイダ 310 から衛星放送などで受信したセキュアコンテンツ 304 を復号モジュール 905 に出力する。また、通信モジュール 162 は、サービスプロバイダ 310 から電話回線などを介して受信したユーザ嗜好フィルタデータ 900 を CAモジュール 311 に出力すると共に、CAモジュール 311 から入力した SP 用購入履歴データ 309 を電話回線などを介してサービスプロバイダ 310 に送信する。

図 75 は、CAモジュール 311 および復号モジュール 905 の機能ブロック図である。

図 75 に示すように、CAモジュール 311 は、相互認証部 906、記憶部 907、暗号化・復号部 908 および SP 用購入履歴データ生成部 909 を有する。

相互認証部 906 は、CAモジュール 311 とサービスプロバイダ 310 との間で電話回線を介してデータを送受信する際に、サービスプロバイダ 310 との間で相互認証を行ってセッション鍵データ K_{ss} を生成し、これを暗号化・復号部 908 に出力する。

記憶部 907 は、例えば、サービスプロバイダ 310 とユーザとの間で契約が成立した後に、サービスプロバイダ 310 から IC カード 912 などを用いてオフラインで供給されたマスタ鍵データ K_M を記憶する。

暗号化・復号部 908 は、復号モジュール 905 の復号部 910 からそれぞれ暗号化されたスクランブル鍵データ K_{scr} およびワーク鍵データ K_w を入力し、記憶部 907 から読み出したマスタ鍵データ K_m を用いてワーク鍵データ K_w を復号する。そして、暗号化・復号部 908 は、当該復号したワーク鍵データ K_w を用いてスクランブル鍵データ K_{scr} を復号し、当該復号したスクランブル鍵データ K_{scr} を復号部 910 に出力する。

また、暗号化・復号部 908 は、電話回線などを介して通信モジュール 162 がサービスプロバイダ 310 から受信したユーザ嗜好フィルタデータ 900 を、相互認証部 906 からのセッション鍵データ K_{ss} を用いて復号して復号モジュール 905 のセキュアコンテナ選択部 911 に出力する。

また、暗号化・復号部 908 は、SP 用購入履歴データ生成部 909 から入力した SP 用購入履歴データ 309 を、相互認証部 906 からのセッション鍵データ K_{ss} を用いて復号して通信モジュール 162 を介してサービスプロバイダ 310 に送信する。

SP 用購入履歴データ生成部 909 は、図 74 に示す購入・利用形態決定操作部 165 を用いてユーザによるコンテンツデータ C の購入操作に応じた操作信号 S165、または SAM305₁ からの利用制御状態データ 166 に基づいて、サービスプロバイダ 310 に固有のコンテンツデータ C の購入履歴を示す SP 用購入履歴データ 309 を生成し、これを暗号化・復号部 908 に出力する。

SP 用購入履歴データ 309 は、例えば、サービスプロバイダ 310 が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

なお、CA モジュール 311 は、サービスプロバイダ 310 が課金機能を有している場合には、サービスプロバイダ 310 の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CA モジュール 311 は、コンテンツデータの配信サービスについての課金データ

をサービスプロバイダ 310 に送信する。

復号モジュール 905 は、復号部 910 およびセキュアコンテナ選択部 911 を有する。

復号部 910 は、通信モジュール 162 から、それぞれ暗号化されたセキュアコンテナ 304、スクランブル鍵データ K_{scr} およびワーク鍵データ K_w を入力する。

そして、復号部 910 は、暗号化されたスクランブル鍵データ K_{scr} およびワーク鍵データ K_w を CA モジュール 311 の暗号化・復号部 908 に出力し、暗号化・復号部 908 から復号されたスクランブル鍵データ K_{scr} を入力する。

そして、復号部 910 は、暗号化されたセキュアコンテナ 304 を、スクランブル鍵データ K_{scr} を用いて復号した後に、セキュアコンテナ選択部 911 に出力する。

なお、セキュアコンテナ 304 が、MPEG2 Transport Stream 方式でサービスプロバイダ 310 から送信される場合には、例えば、復号部 910 は、TS Packet 内の ECM (Entitlement Control Message) からスクランブル鍵データ K_{scr} を取り出し、EMM (Entitlement Management Message) からワーク鍵データ K_w を取り出す。

ECM には、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMM は、その他に、ユーザ（視聴者）毎に異なる個別試験契約情報などが含まれている。

セキュアコンテナ選択部 911 は、復号部 910 から入力したセキュアコンテナ 304 を、CA モジュール 311 から入力したユーザ嗜好フィルタデータ 900 を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ 304 を選択して SAM 305₁ に出力する。

次に、SAM 305₁ について説明する。

なお、SAM 305₁ は、サービスプロバイダ 310 についての署名検証処理

SAM105₁～105₄は、上述したセキュアコンテナ104の購入・利用の履歴を利用履歴(Usage Log)データ108として記録すると共に、購入形態を示す利用制御状態データ166を作成する。

利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

利用制御状態データ166は、例えば、購入形態が決定される度に、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。

また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。

すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局92に対しての(ルート認証局92の下層に位置する)セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ101およびSAM105₁～105₄において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権利書データ106を登録して権威化することも、EMDサービスセンタ102の認証機能の一つである。

また、EMDサービスセンタ102は、例えば、配信用鍵データKD₁～KD_nなどの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP(Suggested Retailer' Price)とSAM105₁～SAM105_nから入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理(利益分配)機能を有する。

図2は、セキュアコンテナ104の概念をまとめた図である。

図2に示すように、セキュアコンテナ104には、コンテンツプロバイダ101が作成したコンテンツファイルCFと、EMDサービスセンタ102が作成したキーファイルKFとが格納されている。

コンテンツファイルCFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、コンテンツ鍵データK_cを用いた暗号化されたコンテンツデータCと、これらについてのコンテンツプロバイダ101の秘密鍵データK_{cp}を用いた署名データとが格納されている。

キーファイルKFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、配信用鍵データKD₁～KD_nによって暗号化されたコンテンツ鍵データK_cおよび権利書データ106と、これらについてのEMDサービスセンタ102の秘密鍵データK_{sc}による署名データとが格納されている。

以下、コンテンツプロバイダ101の各構成要素について詳細に説明する。

(コンテンツプロバイダ101)

図3は、コンテンツプロバイダ101の機能ブロック図であり、ユーザホームネットワーク103のSAM105₁～105_nとの間で送受信されるデータに関連するデータの流れが示されている。

また、図4には、コンテンツプロバイダ101とEMDサービスセンタ102との間で送受信されるデータに関連するデータの流れが示されている。

なお、図4以降の図面では、署名データ処理部、および、セッション鍵データK_{sess}を用いた暗号化・復号部に入出力するデータの流は省略している。

図3および図4に示すように、コンテンツプロバイダ101は、コンテンツマスタソースデータベース111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、伸長部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、キーファイルデータベース118b、記憶部(データベース)119、相互認証部120、暗号化・復号部121、権利書データ作成部122、聴感検査部123、SAM管理部124、EMDサービスセンタ管理部125およびコンテンツID生成部850を有する。

コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号(決済を行う口座番号)をオフラインでEMDサービスセンタ102に登録し、自らの識別子(識別番号)CP_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データと、ルート認証局92の公開鍵データとを受ける。

以下、図3および図4に示すコンテンツプロバイダ101の各機能ブロックについて説明する。

コンテンツマスタソースデータベース111は、ユーザホームネットワーク103に提供するコンテンツのマスタソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータS111を電子透かし情報付加部112に出力する。

電子透かし情報付加部112は、コンテンツデータS111に対して、ソース電子透かし情報(Source Watermark)Ws、コピー管理用電子透かし情報(Copy Control Watermark)Wc、ユーザ電子透かし情報(User Watermark)Wuおよびリンク用電子透かし情報(Link Watermark)WLなどを埋め込んでコンテンツデータS

112を生成し、コンテンツデータS112を圧縮部113に出力する。

ソース電子透かし情報Wsは、コンテンツデータの著作権者名、ISRCコード、オーサリング日付、オーサリング機器ID(Identification Data)、コンテンツの配給先などの著作権に関する情報である。

コピー管理用電子透かし情報Wcは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。

ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP_IDおよびユーザホームネットワーク103のSAM105₁～105₄の識別子SAM_ID₁～SAM_ID₄が含まれる。

リンク用電子透かし情報(Link Watermark)WLは、例えば、コンテンツデータCのコンテンツIDを含んでいる。

リンク用電子透かし情報WLをコンテンツデータCに埋め込むことで、例えば、テレビジョンやAM/FMラジオなどのアナログ放送でコンテンツデータCが配信された場合でも、ユーザからの要求に応じて、EMDサービスセンタ102は、当該コンテンツデータCを扱っているコンテンツプロバイダ101をユーザに紹介できる。すなち、当該コンテンツデータCの受信先において、電子透かし情報デコーダを利用したコンテンツデータCに埋め込まれたリンク用電子透かし情報WLを検出し、当該検出したリンク用電子透かし情報WLに含まれるコンテンツIDをEMDサービスセンタ102に送信することで、EMDサービスセンタ102は当該ユーザに対して、当該コンテンツデータCを扱っているコンテンツプロバイダ101などを紹介できる。

具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコーダが、当該コンテンツデータCに埋め込まれているリンク用電子透かし情報WLに含まれるコンテンツIDや当該コンテンツデータCを

登録しているEMDサービスセンタ102の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやMD(Mini Disk)などの光ディスクなどの可搬メディアに搭載されているメディアSAMに記録する。そして、当該可搬メディアをネットワークに接続されているSAMを搭載したネットワーク機器をセットする。そして、当該SAMとEMDサービスセンタ102とが相互認証を行った後に、メディアSAMに搭載されている個人情報と、上記記録したコンテンツIDなどをネットワーク機器からEMDサービスセンタ102に送信する。その後、ネットワーク機器に、当該コンテンツデータCを扱っているコンテンツプロバイダ101などの紹介リストなどを、EMDサービスセンタ102から受信する。

また、その他に、例えば、EMDサービスセンタ102が、ユーザからコンテンツIDなどを受信したときに、当該コンテンツIDに対応したコンテンツデータCを提供しているコンテンツプロバイダ101に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ101は、当該ユーザが契約者であれば、当該コンテンツデータCをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

なお、後述する第2実施形態では、リンク用電子透かし情報WLに基づいて、EMDサービスセンタ302は、ユーザに、当該コンテンツデータCを扱っているサービスプロバイダ310を紹介できる。

また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールWMとして定義し、EMDサービスセンタ102において電子透かし情報モジュールWMを登録して管理する。電子透かし情報モジュールWMは、例えば、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂～160₄が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク 103 では、EMD サービスセンタ 102 が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

圧縮部 113 は、コンテンツデータ S112 を、例えば、ATRAC3 (Adaptive Transform Acoustic Coding 3) (商標) などの音声圧縮方式で圧縮し、圧縮したコンテンツデータ S113 を暗号化部 114 に出力する。

この場合に、圧縮部 113 による圧縮時に、コンテンツデータに対しての電子透かし情報の埋め込みを再び行ってもよい。具体的には、図 3 に示すように、伸長部 116 においてコンテンツデータ 113 を伸長してコンテンツデータ S116 を生成し、聴感検査部 123 においてコンテンツデータ S116 を再生したときに、電子透かし情報の埋め込みが音質に与える影響を、例えば実際に人間が聴いて判断し、所定の基準を満たさない場合には、電子透かし情報付加部 112 に電子透かし情報の埋め込み処理を再び行うように指示する。

これにより、例えば、データの損失を伴う音声圧縮方式を採用したときに、当該圧縮によって、埋め込んだ電子透かし情報が落ちてしまった場合に適切に対処できる。また、圧縮したコンテンツデータを再度伸長して、埋め込みを行った電子透かし情報を正確に検出できるか否かの確認を行ってもよい。この場合に、音質聴感の検証も行い、聴感上問題がある場合には、電子透かし情報の埋め込みの調整を行う。例えば、マスキング効果を利用して電子透かし情報を埋め込む場合には、電子透かし情報の埋め込みを行うレベルを調整する。

暗号化部 114 は、コンテンツ鍵データ Kc を共通鍵として用い、DES (Data Encryption Standard) や Triple DES などの共通鍵暗号化方式で、コンテンツデータ S113 を暗号化してコンテンツデータ C を生成し、これをセキュアコンテナ作成部 118 に出力する。

また、暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、A/V伸長用ソフトウェアSoft、メタデータMetaおよび電子透かし情報管理データWMを暗号化した後に、セキュアコンテナ作成部117に出力する。

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号化方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）データを共通鍵データから生成する部分（鍵処理部）とからなる。DESの全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の64ビットは、上位32ビットのH₀と下位32ビットのL₀とに分割される。鍵処理部から供給された48ビットの拡大鍵データK₁および下位32ビットのL₀を入力とし、下位32ビットのL₀を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットのH₀と、F関数の出力との排他的論理和が算出され、その結果はL₁とされる。また、L₀は、H₁とされる。

そして、上位32ビットのH₀および下位32ビットのL₀を基に、以上の処理を16回繰り返し、得られた上位32ビットのH₁₆および下位32ビットのL₁₆が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

乱数発生部115は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データKcとして記憶部119に記憶する。

なお、コンテンツ鍵データKcは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データKcは、例えば、所定時間毎に更新される。

また、複数のコンテンツプロバイダ101が存在する場合に、個々のコンテン

ツプロバイダ101によって固有のコンテンツ鍵データKcを用いてもよいし、全てのコンテンツプロバイダ101に共通のコンテンツ鍵データKcを用いてもよい。

キーファイルデータベース118bには、図4に示すように、EMDサービスセンタ管理部125を介してEMDサービスセンタ102から受信した図5(B)に示すキーファイルKFが記憶される。キーファイルKFは、コンテンツデータC毎に存在し、後述するように、コンテンツファイルCFのヘッダ内のディレクトリ構造データDSDによって、対応するコンテンツファイルCFとの間でリンク関係が指定されている。

キーファイルKFには、図5(B)および図7に示すように、ヘッダ、コンテンツ鍵データKc、権利書データ(使用許諾条件)106、SAMプログラム・ダウンロード・コンテナSDC₁～SDC_sおよび署名データSIG_{x1, sec}が格納されている。

ここで、コンテンツプロバイダ101の秘密鍵データK_{sec, s}を用いた署名データは、図5(B)に示すようにキーファイルKFに格納される全てのデータに対しての署名データ_{x1, sec}にしてもよいし、図7に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データKcおよび権利書データ106に対しての署名データと、SAMプログラム・ダウンロード・コンテナSDCに対しての署名データとを別々に設けてもよい。

コンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC_sとは、それぞれ対応する期間の配信用鍵データKD₁～KD_sを用いて暗号化されている。

ヘッダデータには、図7に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データK_{sec, s}による署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイルKFに関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイ

ダ101の秘密鍵データ $K_{\text{asc.}}$ による署名データが含まれる。

なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図8に示すような情報を含めてもよい。

また、コンテンツIDには、例えば、図9に示す情報が含まれている。コンテンツIDは、EMDサービスセンタ102あるいはコンテンツプロバイダ101において作成され、EMDサービスセンタ102において作成された場合には図9に示すようにEMDサービスセンタ102の秘密鍵データ $K_{\text{asc.}}$ による署名データが添付され、コンテンツプロバイダ101において作成された場合にはコンテンツプロバイダ101の秘密鍵データ $K_{\text{cp.}}$ が添付される。

コンテンツIDは、例えば、図4に示すように、コンテンツID生成部850が作成し、記憶部119に格納される。なお、コンテンツIDは、EMDサービスセンタ102が作成してもよい。

ディレクトリ構造データは、セキュアコンテナ104内におけるコンテンツファイルCF相互間の対応関係と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。

例えば、セキュアコンテナ104内にコンテンツファイル $CF_1 \sim CF_n$ と、それらに対応するキーファイル $KF_1 \sim KF_n$ が格納されている場合には、図10に示すように、コンテンツファイル $CF_1 \sim CF_n$ 相互間のリンクと、コンテンツファイル $CF_1 \sim CF_n$ とキーファイル $KF_1 \sim KF_n$ との間のリンク関係とがディレクトリ構造データによって確立される。

ハイパーリンクデータは、セキュアコンテナ104の内外の全てのファイルを対象として、キーファイルKF相互間での階層構造と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。

具体的には、図11に示すように、セキュアコンテナ104内にコンテンツファイルCFおよびキーファイルKF毎のリンク先のアドレス情報とその認証値（

ハッシュ値)とを格納し、ハッシュ関数 $H(x)$ を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

また、権利書データ106には、図7に示すように、コンテンツID、コンテンツプロバイダ101の識別子CP_ID、権利書データ106の有効期限、EMDサービスセンタ102の通信アドレス、利用空間調査情報、卸売価格情報、取扱方針、取扱制御情報、商品デモ(試聴)の取扱制御情報およびそれらについての署名データなどが含まれる。

なお、後述する第2実施形態のように、サービスプロバイダ310を介してユーザホームネットワーク303にセキュアコンテナ304を送信する場合には、権利書データ106には、コンテンツプロバイダ301がセキュアコンテナ104を提供するサービスプロバイダ310の識別子SP_IDが含まれる。

また、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₉には、図7に示すように、SAM105₁～105₄内でプログラムのダウンロードを行なう際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ(UCP)U106のシンタックス(文法)を示すUCP-L(Label)、R(Reader)などのラベルリーダと、SAM105₁～105₄に内蔵された記憶部(フラッシュ-ROM)の書き換えおよび消去をブロック単位でロック状態/非ロック状態にするためのロック鍵データと、それらについての署名データとが含まれる。

なお、記憶部119は、例えば、公開鍵証明書データを記憶するデータベースを含む種々のデータベースを備えている。

署名処理部117は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ101の秘密鍵データK_{CP}を用いて、その署名データSIGを作成する。

なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧

縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

セキュアコンテナ作成部118は、図5（A）に示すように、ヘッダデータと、暗号化部114から入力したそれぞれコンテンツ鍵データKcで暗号化されたメタデータMeta、コンテンツデータC、A/V伸長用ソフトウェアSoftwareおよび電子透かし情報モジュール(Watermark Module)WMとを格納したコンテンツファイルCFを生成する。

コンテンツファイルCFには、図6に示すように、ファイルリーダと、秘密鍵データK_{cs}によるファイルリーダの署名データとを含むようにしてもよい。このようにすることで、SAM105₁～105₄において、異系列の複数のセキュアコンテナ104から受信したそれぞれ異なるフォーマットのコンテンツファイルCFを格納した複数のセキュアコンテナ104を効率的に処理できる。

ここで、ファイルリーダは、コンテンツファイルCFおよびそれに対応するキーファイルKFを読む際に用いられ、これらのファイルの読み込み手順などを示している。

但し、本実施形態では、EMDサービスセンタ102からSAM105₁～105₄に、当該ファイルリーダを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテナ104のコンテンツファイルCFは、ファイルリーダを格納していない。

ヘッダデータには、図6に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データK_{cs}による署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイルCFの有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関しての情報、およびディレクトリ情報な

どに関してのコンテンツプロバイダ101の秘密鍵データ K_{cp} による署名データが含まれる。

メタデータ $Meta$ には、図6に示すように、商品（コンテンツデータ C ）の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ101による署名データが含まれる。

本発明では、図5および図6に示すように、コンテンツファイル CF 内にメタデータ $Meta$ を格納して送信する場合を示す例があるが、メタデータ $Meta$ をコンテンツファイル CF 内に格納せずに、コンテンツファイル CF を送信する経路とは別の経路でコンテンツプロバイダ101から $SAM105$ 、などに送信してもよい。

A/V 伸長用ソフトウェア $Soft$ は、ユーザホームネットワーク103のネットワーク機器160₁および AV 機器160₂～160₄において、コンテンツファイル CF を伸長する際に用いられるソフトウェアであり、例えば、 $ATRAC3$ 方式の伸長用ソフトウェアである。

このように、セキュアコンテナ104内に A/V 伸長用ソフトウェア $Soft$ を格納することで、 $SAM105$ 、～105₄においてセキュアコンテナ104内に格納された A/V 伸長用ソフトウェア $Soft$ を用いてコンテンツデータ C の伸長を行うことができ、コンテンツデータ C 毎あるいはコンテンツプロバイダ101毎にコンテンツデータ C の圧縮および伸長方式をコンテンツプロバイダ101が自由に設定しても、ユーザに多大な負担をかけることはない。

電子透かし情報モジュール WM は、前述したように、例えば、コンテンツデータ C に埋め込まれた電子透かし情報を検出するのに必要は情報およびソフトウェアを含んでいる。

また、セキュアコンテナ作成部118は、上述した図5（A）に示すコンテンツファイル CF と、当該コンテンツファイル CF の署名データ SIG_{cp} と、キーファイルデータベース118bから読み出した当該コンテンツファイル CF に

対応する図5(B)に示すキーファイルKFと、当該キーファイルKFの署名データSIG_{7,cr}と、記憶部119から読み出したコンテンツプロバイダ101の公開鍵証明書データCER_{cr}と、当該公開鍵証明書データCER_{cr}の署名データSIG_{1,ssc}とを格納したセキュアコンテナ104を生成する。

ここで、署名データSIG_{8,cr}は、セキュアコンテナ104の受信先において、コンテンツファイルCFの作成者および送信者の正当性を検証するために用いられる。

ここで、署名データSIG_{7,cr}は、セキュアコンテナ104の受信先において、キーファイルKFの送信者の正当性を検証するために用いられる。なお、セキュアコンテナ104の受信先において、キーファイルKFの作成者の正当性の検証は、キーファイルKF内の署名データSIG_{1,ssc}に基づいて行われる。また、署名データSIG_{1,ssc}は、キーファイルKFが、EMDサービスセンタ102に登録されているか否かを検証するためにも用いられる。

本実施形態では、コンテンツデータCの圧縮方式、圧縮の有無、暗号化方式（共通鍵暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータCを得た信号の諸元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータCがセキュアコンテナ104内に格納されている。すなわち、これらの事項をコンテンツプロバイダ101が自由に決定できる。

また、セキュアコンテナ作成部118は、セキュアコンテナデータベース118aに格納したセキュアコンテナ104を、ユーザからの要求に応じてSAM管理部124に出力する。

このように、本実施形態では、コンテンツプロバイダ101の公開鍵データK_{cr,r}の公開鍵証明書CER_{cr}をセキュアコンテナ104に格納してユーザホームネットワーク103に送信するイン・バンド(In-band)方式を採用している。従って、ユーザホームネットワーク103は、公開鍵証明書CER_{cr}を得るための

通信をEMDサービスセンタ102との間で行う必要がない。

なお、本発明では、公開鍵証明書 CER_{cp} をセキュアコンテナ104に格納しないで、ユーザホームネットワーク103がEMDサービスセンタ102から公開鍵証明書 CER_{cp} を得るアウト・オブ・バンド(Out-Of-band)方式を採用してもよい。

相互認証部120は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103との間でオンラインでデータを送受信する際に、それぞれEMDサービスセンタ102およびユーザホームネットワーク103との間で相互認証を行ってセッション鍵データ(共有鍵) K_{ss} を生成する。セッション鍵データ K_{ss} は、相互認証を行う度に新たに生成される。

暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103にオンラインで送信するデータを、セッション鍵データ K_{ss} を用いて暗号化する。

また、暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103からオンラインで受信したデータを、セッション鍵データ K_{ss} を用いて復号する。

権利書データ作成部122は、権利書データ106を作成し、これをEMDサービスセンタ管理部125に出力する。

権利書データ106は、コンテンツデータCの運用ルールを定義した記述子(ディスクリプター)であり、例えば、コンテンツプロバイダ101の運用者が希望する標準小売価格SRP(Suggested Retailer' Price)やコンテンツデータCの複製ルールなどが記述されている。

SAM管理部124は、セキュアコンテナ104を、オフラインおよび/またはオンラインでユーザホームネットワーク103に供給する。

また、SAM管理部124は、セキュアコンテナ104をオンラインでSAM

105₁～105₄に配給する場合には、セキュアコンテナ104を送信する通信プロトコルとして、デジタル放送であればMHEG(Multimedia and Hypermedia information coding Experts Group)プロトコルを用い、インターネットであればXML/SMIL/HTML(Hyper TextMarkup Language)を用い、これらの通信プロトコル内に、セキュアコンテナ104を、符号化方式に依存しない形式でトンネリングして埋め込む。

従って、通信プロトコルとセキュアコンテナ104との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ104のフォーマットを柔軟に設定できる。

なお、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を送信する際に用いる通信プロトコルは、上述したものには限定されず任意である。

図12は、本実施形態で用いられるROM型の記録媒体130₁を説明するための図である。

図12に示すように、ROM型の記録媒体130₁は、ROM領域131、セキュアRAM領域132およびメディアSAM133を有する。

ROM領域131には、図5(A)に示したコンテンツファイルCFが記憶されている。

また、セキュアRAM領域132は、記憶データに対してのアクセスに所定の許可(認証)が必要な領域であり、図5(B)、(C)に示したキーファイルKFおよび公開鍵証明書データCER_{CP}と機器の種類に応じて固有の値を持つ記録用鍵データK_{STR}とを引数としてMAC(Message Authentication Code)関数を用いて生成した署名データと、当該キーファイルKFおよび公開鍵証明書データCER_{CP}とを記録媒体に固有の値を持つメディア鍵データK_{MD}を用いて暗号化したデータとが記憶される。

また、セキュアRAM領域132には、例えば、不正行為などで無効となった

コンテンツプロバイダ101およびSAM105₁～105₄を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。

また、セキュアRAM領域132には、後述するようにユーザホームネットワーク103のSAM105₁～105₄においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態（UCS）データ166などが記憶される。これにより、利用制御状態データ166がセキュアRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体130₁となる。

メディアSAM133には、例えば、ROM型の記録媒体130₁の識別子であるメディアIDと、メディア鍵データK_{med}とが記憶されている。

メディアSAM133は、例えば、相互認証機能を有している。

本実施形態で用いるROM型の記録媒体としては、例えば、図12に示すもの他に、図13に示すROM型の記録媒体130₂および図14に示すROM型の記録媒体130₃なども考えられる。

図13に示すROM型の記録媒体130₂は、ROM領域131と認証機能を有するメディアSAM133とを有し、図12に示すROM型の記録媒体130₁のようにセキュアRAM領域132を備えていない。ROM型の記録媒体130₂を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。

また、図14に示すROM型の記録媒体130₃は、ROM領域131およびセキュアRAM領域132を有し、図12に示すROM型の記録媒体130₁のようにメディアSAM133を有していない。ROM型の記録媒体130₃を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記録する。また、ROM型の記録媒体130₃を用いる場合には、SAMとの間で相互認証は行わない。

また、本実施形態ではROM型の記録媒体の他にRAM型の記録媒体も用いら

れる。

本実施形態で用いるRAM型の記録媒体としては、例えば図15に示すように、メディアSAM133、セキュアRAM領域132およびセキュアでないRAM領域134を有するRAM型の記録媒体130₄がある。RAM型の記録媒体130₄では、メディアSAM133は認証機能を持ち、キーファイルKFを記憶する。また、RAM領域134には、コンテンツファイルCFが記録される。

また、本実施形態で用いるRAM型の記録媒体としては、その他に、図16に示すRAM型の記録媒体135₀、および図17に示すRAM型の記録媒体130₀なども考えられる。

図16に示すRAM型の記録媒体130₀は、セキュアでないRAM領域134と認証機能を有するメディアSAM133とを有し、図15に示すRAM型の記録媒体130₄のようにセキュアRAM領域132を備えていない。RAM型の記録媒体130₀を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。

また、図17に示すRAM型の記録媒体130₀は、セキュアRAM領域132およびセキュアでないRAM領域134を有し、図15に示すRAM型の記録媒体130₄のようにメディアSAM133を有していない。RAM型の記録媒体130₀を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記録する。また、RAM型の記録媒体130₀を用いる場合には、SAMとの間で相互認証は行わない。

また、SAM管理部124は、セキュアコンテナ104を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク103に配信する場合には、暗号化・復号部121においてセッション鍵データK_{ss}を用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してユーザホーム

ネットワーク 103 に配信する。

本実施形態では、SAM管理部、EMDサービスセンタ管理部、並びに後述するコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

ここで、コンテンツプロバイダ 101 からユーザホームネットワーク 103 へのコンテンツデータ C の配給は、上述したように記録媒体 130₁ を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ 106 が格納された共通の形式のセキュアコンテナ 104 を用いる。従って、ユーザホームネットワーク 103 の SAM 105₁ ~ 105₄ では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ 106 に基づいた権利処理を行なうことができる。

また、上述したように、本実施形態では、セキュアコンテナ 104 内に、コンテンツ鍵データ Kc で暗号化されたコンテンツデータ C と、当該暗号化を解くためのコンテンツ鍵データ Kc とを同封するイン・バンド(In-Band)方式を採用している。イン・バンド方式では、ユーザホームネットワーク 103 の機器で、コンテンツデータ C を再生しようとするときに、コンテンツ鍵データ Kc を別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データ Kc は配信用鍵データ KD₁ ~ KD₄ で暗号化されているが、配信用鍵データ KD₁ ~ KD₄ は、EMDサービスセンタ 102 で管理されており、ユーザホームネットワーク 103 の SAM 105₁ ~ 105₄ に事前（SAM 105₁ ~ 105₄ が EMD サービスセンタ 102 に初回にアクセスする際に）配信されているので、ユーザホームネットワーク 103 では、EMD サービスセンタ 102 との間をオンラインで接続することなく、オフラインで、コンテンツデータ C の利用が可能になる。

なお、本発明は、後述するようにコンテンツデータ C とコンテンツ鍵データ K

cとを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band)方式を採用できる柔軟性を有している。

EMDサービスセンタ管理部125は、EMDサービスセンタ102から決済レポートデータ107を受信すると、これらを暗号化・復号部121においてセッション鍵データ K_{ss} を用いて復号した後に、記憶部119に記憶する。

決済レポートデータ107は、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

また、EMDサービスセンタ管理部125は、提供するコンテンツデータCのグローバルユニーク(Global Unique)な識別子であるコンテンツID、公開鍵データ $K_{cp, p}$ およびそれらの署名データ $SIG_{s, cp}$ を、EMDサービスセンタ102に送信し、EMDサービスセンタ102から、公開鍵データ $K_{cp, p}$ の公開鍵証明書データ CER_{cp} を入力する。

また、EMDサービスセンタ管理部125は、コンテンツデータCのそれぞれについて、コンテンツ鍵データ K_c 、権利書データ106および電子透かし情報管理データWMをEMDサービスセンタ102に登録してキーファイルKFを受け取る際に、図18に示すように、提供するコンテンツデータCのグローバルユニークな識別子であるコンテンツID、コンテンツ鍵データ K_c 、権利書データ106、電子透かし情報管理データWM、コンテンツプロバイダ101のグローバルユニークな識別子であるCP_IDと、それらについてのコンテンツプロバイダ101の秘密鍵データ $K_{cp, s}$ による署名データ $SIG_{mi, cp}$ とを格納した登録モジュール Mod_2 を作成する。そして、EMDサービスセンタ管理部125は、登録モジュール Mod_2 を暗号化・復号部121においてセッション鍵データ K_{ss} を用いて暗号化した後に、ネットワークを介してEMDサービスセンタ102に送信する。EMDサービスセンタ管理部125としては、前述したように、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは

困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

以下、図3および図4を参照しながら、コンテンツプロバイダ101における処理の流れを説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニークな識別子CP_IDを得ている。識別子CP_IDは、記憶部119に記憶されている。

まず、コンテンツプロバイダ101が、EMDサービスセンタ102に、自らの秘密鍵データK_{cp,s}に対応する公開鍵データK_{cp,p}の正当性を証明する公開鍵証明書データCER_{cp}を要求する場合の処理を図4を参照しながら説明する。

コンテンツプロバイダ101は、真性乱数発生器を用いて乱数を発生して秘密鍵データK_{cp,s}を生成し、当該秘密鍵データK_{cp,s}に対応する公開鍵データK_{cp,p}を作成して記憶部119に記憶する。

EMDサービスセンタ管理部125は、コンテンツプロバイダ101の識別子CP_IDおよび公開鍵データK_{cp,p}を記憶部119から読み出す。

そして、EMDサービスセンタ管理部125は、識別子CP_IDおよび公開鍵データK_{cp,p}を、EMDサービスセンタ102に送信する。

そして、EMDサービスセンタ管理部125は、当該登録に応じて、公開鍵証明書データCER_{cp}およびその署名データSIG_{1,ss}をEMDサービスセンタ102から入力して記憶部119に書き込む。

次に、コンテンツプロバイダ101が、EMDサービスセンタ102にコンテンツ鍵データK_c、権利書データ106および電子透かし情報管理データWMを登録し、コンテンツデータCに対応するキーファイルKFを受信する場合の処理を図4、図18および図19を参照して説明する。

権利書データ106などの登録は、個々のコンテンツデータCについてそれぞ

れ行われる。

図19は、コンテンツプロバイダ101からEMDサービスセンタ102への登録処理を説明するためのフローチャートである。

ステップA1：図4に示すコンテンツプロバイダ101の相互認証部120とEMDサービスセンタ102との間で相互認証を行う。

ステップA2：ステップA1で行った相互認証によって得られたセッション鍵データ K_{ss} をコンテンツプロバイダ101およびEMDサービスセンタ102で共有する。

ステップA3：コンテンツプロバイダ101は、記憶部119などのデータベースから、EMDサービスセンタ102に登録を行うコンテンツID、コンテンツ鍵データ K_c 、権利書データ106、電子透かし情報管理データWMおよびCP_IDなどを読み出す。

ステップA4：署名処理部117において、コンテンツプロバイダ101の秘密鍵データ K_{cp} を用いて、ステップA3で読み出した権利書データ106などを含むモジュールに対して、送り主の正当性を示す署名データSIG_{ml}を作成する。

そして、EMDサービスセンタ管理部125は、図18に示すように、コンテンツID、コンテンツ鍵データ K_c 、権利書データ106、電子透かし情報管理データWMおよびCP_IDと、これらについての署名データSIG_{ml}とを格納した登録用モジュールMod₂を作成する。

ステップA5：暗号化・復号部121は、ステップA4で作成した登録用モジュールMod₂を、ステップA2で共有したセッション鍵データ K_{ss} を用いて暗号化する。

ステップA6：EMDサービスセンタ管理部125は、ステップA5で暗号化した登録用モジュールMod₂をEMDサービスセンタ102に送信する。

ステップA7以降の処理は、EMDサービスセンタ102における処理である

。

ステップA7: EMDサービスセンタ102は、受信した登録用モジュールMod₂を、ステップA2において共有したセッション鍵データK_{ss}を用いて復号する。

ステップA8: EMDサービスセンタ102は、復号した登録用モジュールMod₂に格納された署名データSIG_{M1,ss}を公開鍵データK_{cp,p}を用いて検証し、登録用モジュールMod₂の送り主の正当性を確認し、送り主の正当性が証明されたことを条件にステップA9の処理を行う。

ステップA9: EMDサービスセンタ102は、登録用モジュールMod₂に格納されているコンテンツID、コンテンツ鍵データK_c、権利書データ106、電子透かし情報管理データWMおよびCP_IDを所定のデータベースに格納して登録する。

なお、EMDサービスセンタ管理部125は、図18に示すように、登録用モジュールMod₂に応じた登録処理がEMDサービスセンタ102に行われた後に、例えば6カ月分のキーファイルKFをEMDサービスセンタ102から受信し、相互認証部120とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データK_{ss}を用いて、当該受信したキーファイルKFを復号した後、キーファイルデータベース118bに記憶する。

次に、コンテンツプロバイダ101がユーザホームネットワーク103のSAM105₁にセキュアコンテナ104を送信する場合の処理を図3および図4を参照しながら説明する。

なお、以下の例では、コンテンツプロバイダ101からSAM105₁にセキュアコンテナ104を送信する場合を例示するが、セキュアコンテナ104をSAM105₂～105₄に送信する場合も、SAM105₁を介してSAM105₂～105₄に送信される点を除いて同じである。

先ず、図3に示すように、コンテンツデータS111がコンテンツマスター

データベース 111 から読み出されて電子透かし情報付加部 112 に出力される。

次に、電子透かし情報付加部 112 は、コンテンツデータ S111 に電子透かし情報を埋め込んでコンテンツデータ S112 を生成し、これを圧縮部 113 に出力する。

次に、圧縮部 113 は、コンテンツデータ S112 を、例えば ATRAC3 方式で圧縮してコンテンツデータ S113 を作成し、これを暗号化部 114 に出力する。

また、図 4 に示すように、乱数発生部 115 において、乱数を発生してコンテンツ鍵データ Kc が生成され、当該生成されたコンテンツ鍵データ Kc が記憶部 119 に記憶される。

次に、暗号化部 114 は、圧縮部 113 から入力したコンテンツデータ S113 と、記憶部 119 から読み出したメタデータ Meta、A/V 伸長用ソフトウェア Software および電子透かし情報管理データ WM とを、コンテンツ鍵データ Kc を用いて暗号化してセキュアコンテナ作成部 118 に出力する。この場合に、メタデータ Meta および電子透かし情報管理データ WM は暗号化しなくてもよい。

そして、セキュアコンテナ作成部 118 は、図 5 (A) に示すコンテンツファイル CF を作成する。また、署名処理部 117 において、コンテンツファイル CF のハッシュ値がとられ、秘密鍵データ K_{cr,s} を用いて署名データ S_{IG,s,cr} が生成される。

また、セキュアコンテナ作成部 118 は、キーファイルデータベース 118b から、コンテンツデータ C に対応するキーファイル KF を読み出し、これを署名処理部 117 に出力する。

そして、署名処理部 117 は、セキュアコンテナ作成部 118 から入力したキーファイル KF のハッシュ値をとり、秘密鍵データ K_{cr,s} を用いて署名データ S

IG_{7.cr}を生成し、これをセキュアコンテナ作成部118に出力する。

次に、セキュアコンテナ作成部118は、図5(A)に示すコンテンツファイルCFおよびその署名データSIG_{4.cr}と、図5(B)に示すキーファイルKFおよびその署名データSIG_{7.cr}と、記憶部119から読み出した図5(C)に示す公開鍵証明書データCER_{cr}およびその署名データSIG_{1.sso}とを格納したセキュアコンテナ104を作成し、これを、セキュアコンテナデータベース118aに記憶する。そして、セキュアコンテナ作成部118は、例えばユーザからの要求(リクエスト)に応じてユーザホームネットワーク103に提供しようとするセキュアコンテナ104をセキュアコンテナデータベース118aから読み出して、相互認証部120とSAM105₁との間の相互認証によって得られたセッション鍵データK_{ss}を用いて暗号化・復号部121において暗号化した後に、SAM管理部124を介してユーザホームネットワーク103のSAM105₁に送信する。

以下、コンテンツプロバイダ101の処理の全体の流れの概要を、セキュアコンテナ作成処理と関連付けて述べる。

図20、図21、図22は、当該処理の流れを説明するためのフローチャートである。

ステップB1: コンテンツプロバイダ101は、予め自らの公開鍵証明書データCER_{cr}をEMDサービスセンタ102から入力し、記憶部(データベース)119に格納しておく。

ステップB2: 新しくオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスタソースをデジタル化し、さらにコンテンツIDを割り振り、コンテンツマスタソースデータベース111に格納して一元的に管理する。

ステップB3: ステップB1において一元的に管理した各々のコンテンツマスタソースにメタデータMetaを作成し、これを記憶部119に格納する。

ステップB4：コンテンツマスタソースデータベース111からコンテンツマスタソースであるコンテンツデータS111を読み出して電子透かし情報付加部112に出力し、電子透かし情報を埋め込んでコンテンツデータS112を生成する。

ステップB5：電子透かし情報付加部112は、埋め込みを行った電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップB6：圧縮部113において、電子透かし情報が埋め込まれたコンテンツデータS112を圧縮してコンテンツデータS113を生成する。

ステップB7：伸長部116において、圧縮されたコンテンツデータS113を伸長してコンテンツデータS116を生成する。

ステップB8：聴感検査部123において、伸長したコンテンツデータS116の聴感検査を行う。

ステップB9：コンテンツプロバイダ101は、コンテンツデータS116に埋め込まれた電子透かし情報を、ステップB5でデータベースに格納した埋め込み内容および埋め込み位置に基づいて検出する。

そして、コンテンツプロバイダ101は、聴感検査および電子透かし情報の検出の双方が成功した場合には、ステップB10の処理を行い、何れか一方が失敗した場合にはステップB4の処理を繰り返す。

ステップB10：乱数発生部115において乱数してコンテンツ鍵データKcを生成し、これを記憶部119に格納する。

ステップB11：暗号化部114において、圧縮したコンテンツデータS113を、コンテンツ鍵データKcを用いて暗号化してコンテンツデータCを作成する。

ステップB12：権利書データ作成部122において、コンテンツデータCについての権利書データ106を作成する。

ステップB13：コンテンツプロバイダ101は、SRPを決定し、これを記

憶部119に格納する。

ステップB14:コンテンツプロバイダ101は、コンテンツID、コンテンツ鍵データKcおよび権利書データ106をEMDサービスセンタ102に出力する。

ステップB15:コンテンツプロバイダ101は、配信用鍵データKD₁〜KD_Dで暗号化されたキーファイルKFをEMDサービスセンタ102から入力する。

ステップB16:コンテンツプロバイダ101は、入力したキーファイルKFをキーファイルデータベース118bに格納する。

ステップB17:コンテンツプロバイダ101は、コンテンツデータCとキーファイルKFとのリンク関係をハイパーリンクで結ぶ。

ステップB18:署名処理部117において、コンテンツデータCおよびキーファイルKFの各々について、秘密鍵データK_{CP}を用いて、作成者の正当性を署名データを作成する。

ステップA19:セキュアコンテナ作成部118において、図5に示すセキュアコンテナ104を作成する。

ステップB20:複数のセキュアコンテナを用いたコンポジット形式でコンテンツデータを提供する場合には、ステップB1〜A19の処理を繰り返して各々のセキュアコンテナ104を作成し、コンテンツファイルCFとキーファイルKFとの間のリンク関係と、コンテンツファイルCF相互間のリンク関係をハイパーリンクなどを用いて結ぶ。

ステップB21:コンテンツプロバイダ101は、作成したセキュアコンテナ104をセキュアコンテナデータベース118aに格納する。

(EMDサービスセンタ102)

EMDサービスセンタ102は、認証(CA:Certificate Authority)機能、鍵管理(Key Management)機能および権利処理(Rights Clearing) (利益分配)機

能を有する。

図23は、EMDサービスセンタ102の機能の構成図である。

図23に示すように、EMDサービスセンタ102は、鍵サーバ141、鍵データベース141a、決算処理部142、署名処理部143、決算機関管理部144、証明書・権利書管理部145、権利書データベース145a、証明書データベース145b、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150、暗号化・復号部151およびKF作成部153を有する。

なお、図23には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ101との間で送受信されるデータに関連するデータの流れが示されている。

また、図24には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、SAM105₁～105₄および図1に示す決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

鍵サーバ141は、鍵データベース141aに記憶された各々有効期間が1カ月の配信用鍵データを要求に応じて6か月分読み出してSAM管理部149に出力する。

また、鍵データベース141a配信用鍵データKDの他に、EMDサービスセンタ102の秘密鍵データK_{ESC,s}、記録用鍵データK_{STR}、メディア鍵データK_{MD}およびMAC鍵データK_{MAC}などの鍵データを記憶する一連の鍵データを格納している。

決算処理部142は、SAM105₁～105₄から入力した利用履歴データ108と、証明書・権利書管理部145から入力した標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済レポートデータ107および決済請求権データ152を作成し、決済レポートデータ107をコンテンツプロバイダ管理部148に出力し、決済請求権データ152を決算機関管理部144

に出力する。

なお、決算処理部142は、販売価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。

ここで、利用履歴データ108は、ユーザホームネットワーク103におけるセキュアコンテナ104の購入、利用（再生、記録および転送など）の履歴を示し、決算処理部142においてセキュアコンテナ104に関連したライセンス料の支払い額を決定する際に用いられる。

利用履歴データ108には、例えば、セキュアコンテナ104に格納されたコンテンツデータCの識別子であるコンテンツID、セキュアコンテナ104を配給したコンテンツプロバイダ101の識別子CP_ID、セキュアコンテナ104内のコンテンツデータCの圧縮方法、セキュアコンテナ104を記録した記録媒体の識別子Media_ID、セキュアコンテナ104を配給を受けたSAM105₁～105_nの識別子SAM_ID、当該SAM105₁～105_nのユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率表は、例えば、セキュアコンテナ104に格納されたコンテンツデータ毎に作成される。

また、決済請求権データ152は、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

なお、決済機関91は、決済が終了すると、当該決済機関の利用明細書をEMDサービスセンタ102に送る。EMDサービスセンタ102は、当該利用明細書の内容を、対応する権利者に通知する。

決算機関管理部144は、決算処理部142が生成した決済請求権データ152を図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。

なお、後述するように、決算機関管理部144は、決済請求権データ152を、コンテンツプロバイダ101などの権利者に送信し、受信した決済請求権データ152を用いて、権利者自らが決済機関91に対しての決済を行ってもよい。

また、決算機関管理部144は、署名処理部143において決済請求権データ152のハッシュ値をとり、秘密鍵データ $K_{sec.}$ を用いて生成した署名データ SIG_{ss} を決済請求権データ152と共に決済機関91に送信する。

証明書・権利書管理部145は、証明書データベース145bに登録（記録）されて権威化された公開鍵証明書データ CER_{cp} および公開鍵証明書データ $CER_{sam1} \sim CER_{sam4}$ などを読み出すと共に、コンテンツプロバイダ101の権利書データ106、コンテンツ鍵データ K_c および電子透かし情報管理データ WM などを権利書データベース145aに登録して権威化する。

ここで、権利書データベース145aはコンテンツIDを検索キーとして検索が行われ、証明書データベース145bはコンテンツプロバイダ101の識別子 CP_ID を検索キーとして検索が行われる。

また、証明書・権利書管理部145は、例えば、権利書データ106、コンテンツ鍵データ K_c および電子透かし情報管理データ WM などのハッシュ値をとり、秘密鍵データ $K_{sec.}$ を用いた署名データを付した権威化されたデータを権利書データベース145aに格納する。

コンテンツプロバイダ管理部148は、コンテンツプロバイダ101との間で通信する機能を有し、登録されたコンテンツプロバイダ101の識別子 CP_ID などを管理する CP データベース148aにアクセスできる。

SAM 管理部149は、ユーザホームネットワーク103内の $SAM105$ 、

～105₄との間で通信する機能を有し、登録されたSAMの識別子SAM_IDやSAM登録リストなどを記録したSAMデータベース149aにアクセスできる。

KF作成部153は、コンテンツプロバイダ管理部148から入力したコンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃とを署名処理部143に出力する。

また、KF作成部153は、鍵サーバ141から入力した対応する期間の配信用鍵データKD₁～KD₃を用いて、コンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₃を暗号化し、図5(B)に示すように、当該暗号化したデータと、署名処理部143から入力した当該暗号化したデータについての秘密鍵データK_{esc.s}による署名データSIG_{K1,esc}とを格納したキーファイルKFを作成し、当該作成したキーファイルKFをKFデータベース153aに格納する。

以下、EMDサービスセンタ102内での処理の流れを説明する。

まず、EMDサービスセンタ102からユーザホームネットワーク103内のSAM105₁～105₄に配信用鍵データを送信する際の処理の流れを、図24を参照しながら説明する。

図24に示すように、鍵サーバ141は、所定期間毎に、例えば、3カ月分の配信用鍵データKD₁～KD₃を鍵データベース141aから読み出してSAM管理部149に出力する。

また、署名処理部143は、配信用鍵データKD₁～KD₃の各々のハッシュ値を取り、EMDサービスセンタ102の秘密鍵データK_{esc.s}を用いて、それぞれに対応する署名データSIG_{KD1,esc}～SIG_{KD3,esc}を作成し、これをSAM管理部149に出力する。

SAM管理部149は、この3カ月分の配信用鍵データKD₁～KD₃およびそれらの署名データSIG_{KD1,esc}～SIG_{KD3,esc}を、相互認証部150とS

AM105₁～105₄と間の相互認証で得られたセッション鍵データK_{ss}を用いて暗号化した後に、SAM105₁～105₄に送信する。

次に、EMDサービスセンタ102がコンテンツプロバイダ101から、公開鍵証明書データCER_{cp}の発行要求を受けた場合の処理を、図23を参照しながら説明する。

この場合に、コンテンツプロバイダ管理部148は、コンテンツプロバイダ101の識別子CP_ID、公開鍵データK_{cp}および署名データSIG_{s, cp}をコンテンツプロバイダ101から受信すると、これらを、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{ss}を用いて復号する。

そして、当該復号した署名データSIG_{s, cp}の正当性を署名処理部143において確認した後に、識別子CP_IDおよび公開鍵データK_{cp}に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ101がCPデータベース148aに登録されているか否かを確認する。

そして、証明書・権利書管理部145は、当該コンテンツプロバイダ101の公開鍵証明書データCER_{cp}を証明書データベース145bから読み出してコンテンツプロバイダ管理部148に出力する。

また、署名処理部143は、公開鍵証明書データCER_{cp}のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{esc}を用いて、署名データSIG_{i, esc}を作成し、これをコンテンツプロバイダ管理部148に出力する。

そして、コンテンツプロバイダ管理部148は、公開鍵証明書データCER_{cp}およびその署名データSIG_{i, esc}を、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{ss}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

次に、EMDサービスセンタ102がSAM105₁から、公開鍵証明書データCER_{sAM1}の発行要求を受けた場合の処理を、図24を参照しながら説明する

。

この場合に、SAM管理部149は、SAM105₁の識別子SAM₁ __ID、公開鍵データK_{SAM1.P}および署名データSIG_{S.SAM1}をSAM105₁から受信すると、これらを、相互認証部150とSAM105₁と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。

そして、当該復号した署名データSIG_{S.SAM1}の正当性を署名処理部143において確認した後に、識別子SAM₁ __IDおよび公開鍵データK_{SAM1.P}に基づいて、当該公開鍵証明書データの発行要求を出したSAM105₁がSAMデータベース149aに登録されているか否かを確認する。

そして、証明書・権利書管理部145は、当該SAM105₁の公開鍵証明書データCER_{SAM1}を証明書データベース145bから読み出してSAM管理部149に出力する。

また、署名処理部143は、公開鍵証明書データCER_{SAM1}のハッシュ値を取り、EMDサービスセンタ102の秘密鍵データK_{SEC.S}を用いて、署名データSIG_{S.S.SEC}を作成し、これをSAM管理部149に出力する。

そして、SAM管理部149は、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{S.S.SEC}を、相互認証部150とSAM105₁と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、SAM105₁に送信する。

なお、SAM105₂～105₄が、公開鍵証明書データを要求した場合の処理は、対象がSAM105₂～105₄に代わるのみで、基本的に上述したSAM105₁の場合と同じである。

なお、本発明では、EMDサービスセンタ102は、例えば、SAM105₁の出荷時に、SAM105₁の秘密鍵データK_{SAM1.S}および公開鍵データK_{SAM1.P}をSAM105₁の記憶部に記憶する場合には、当該出荷時に、公開鍵データK_{SAM1.P}の公開鍵証明書データCER_{SAM1}を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データ CER_{SAM1} を、 $SAM1051$ の記憶部に記憶してもよい。

次に、EMDサービスセンタ102が、コンテンツプロバイダ101から図18に示す登録用モジュール Mod_2 を受けた場合の処理を、図23を参照しながら説明する。

この場合には、コンテンツプロバイダ管理部148がコンテンツプロバイダ101から図18に示す登録用モジュール Mod_2 を受信すると、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{ss} を用いて登録用モジュール Mod_2 を復号する。

そして、署名処理部143において、鍵データベース141aから読み出した公開鍵データ K_{ep} を用いて、署名データ $SIG_{K1, ep}$ の正当性を検証する。

次に、証明書・権利書管理部145は、登録用モジュール Mod_2 に格納された権利書データ106、コンテンツ鍵データ Kc 、電子透かし情報管理データ WM および SRP を、権利書データベース145aに登録する。

次に、コンテンツプロバイダ管理部148は、コンテンツ鍵データ Kc および権利書データ106を KF 作成部153に出力する。

次に、 KF 作成部153は、コンテンツプロバイダ管理部148から入力したコンテンツ鍵データ Kc および権利書データ106と、 SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_9$ とを署名処理部143に出力する。

そして、署名処理部143は、 KF 作成部153から入力したデータ全体に対してハッシュ値をとり、EMDサービスセンタ102の秘密鍵データ $K_{esc, s}$ を用いて、その署名データ $SIG_{K1, esc}$ を作成し、これを KF 作成部153に出力する。

次に、 KF 作成部153において、鍵サーバ141から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_9$ を用いて、コンテンツ鍵データ Kc および権利書データ106と、 SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_9$

C₁を暗号化し、当該暗号化したデータと、署名処理部143から入力した署名データSIG_{K1,ESC}とを格納したキーファイルKFを作成し、これをKFデータベース153aに格納する。

ここで、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃は、登録用モジュールMod₂内に格納したものをを用いても、あるいはEMDサービスセンタ102が予め保持しているものをを用いてもよい。

次に、コンテンツプロバイダ管理部148は、KFデータベース153aにアクセスを行って得たキーファイルKFを、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SE}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

次に、EMDサービスセンタ102において行なう決済処理を図24を参照しながら説明する。

SAM管理部149は、ユーザホームネットワーク103の例えばSAM105₁から利用履歴データ108およびその署名データSIG_{200,SAM1}を入力すると、利用履歴データ108および署名データSIG_{200,SAM1}を、相互認証部150とSAM105₁との間の相互認証によって得られたセッション鍵データK_{SE}を用いて復号し、SAM105₁の公開鍵データK_{SAM1}による署名データSIG_{200,SAM1}の検証を行なった後に、決算処理部142に出力する。

そして、決算処理部142は、SAM管理部149から入力した利用履歴データ108と、証明書・権利書管理部145を介して権利書データベース145aから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。

決算処理部142は、決済請求権データ152を決算機関管理部144に出力すると共に、決済レポートデータ107をコンテンツプロバイダ管理部148に出力する。

次に、決算機関管理部144は、決済請求権データ152およびその署名データSIG_{ss}を、相互認証およびセッション鍵データK_{ss}による復号を行なった後に、図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152に示される金額の金銭が、コンテンツプロバイダ101に支払われる。

次に、EMDサービスセンタ102がコンテンツプロバイダ101に決済レポートを送信する場合の処理を図23を参照しながら説明する。

決算処理部142において決済が行なわれると、前述したように、決算処理部142からコンテンツプロバイダ管理部148に決済レポートデータ107が出力される。

決済レポートデータ107は、上述したように、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

EMDサービスセンタ102は、決算処理部142から決済レポートデータ107を入力すると、これを、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{ss}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

また、EMDサービスセンタ102は、前述したように、権利書データ106を登録（権威化）した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、権威化証明書モジュールを配信用鍵データKD₁～KD_nで暗号化して送信してもよい。

また、EMDサービスセンタ102は、その他に、SAM105₁～105_nの出荷時の処理と、SAM登録リストの登録処理を行なうが、これらの処理については後述する。

〔ユーザホームネットワーク103〕

ユーザホームネットワーク103は、図1に示すように、ネットワーク機器160₁ およびA/V機器160₂～160₄を有している。

ネットワーク機器160₁は、SAM105₁を内蔵している。また、AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。

SAM105₁～105₄の相互間は、例えば、IEEE1394シリアルインタフェースバスなどのバス191を介して接続されている。

なお、AV機器160₂～160₄は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器160₁のネットワーク通信機能を利用してよい。

また、ユーザホームネットワーク103は、ネットワーク機能を有していないAV機器のみを有していてもよい。

以下、ネットワーク機器160₁について説明する。

図25は、ネットワーク機器160₁の構成図である。

図25に示すように、ネットワーク機器160₁は、SAM105₁、通信モジュール162、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。

SAM105₁～105₄は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ102との間で通信を行う。

SAM105₁～105₄は、例えば、EMDサービスセンタ102によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁～105₄のIC(Integrated Circuit)の内部の仕様を知ることはできず、EMDサービスセンタ102が当該ICのインタフェースなどを統一化し、それに従ってネット

ワーク機器160₁ およびAV機器160₂～160₄に搭載される。

SAM105₁～105₄は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Resistant)性を持ったハードウェアモジュール(ICモジュールなど)である。

SAM105₁～105₄の機能をICという形で実現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

以下、SAM105₁の機能について詳細に説明する。

なお、SAM105₂～105₄は、SAM105₁と基本的に同じ機能を有している。

図26は、SAM105₁の機能の構成図である。

なお、図26には、コンテンツプロバイダ101からのセキュアコンテンツ104を入力し、セキュアコンテンツ104内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図26に示すように、SAM105₁は、相互認証部170、暗号化・復号部171、172、173、コンテンツプロバイダ管理部180、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテンツ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、課金処理部187、署名処理部189、SAM管理部190、メディアSAM管理部197、スタック(作業)メモリ200および外部メモリ管理部811を有する。

なお、AV機器160₂～160₄はダウンロードメモリ167を有していないため、SAM105₂～105₄にはダウンロードメモリ管理部182は存在

しない。

なお、図26に示すSAM105₁の所定の機能は、例えば、図示しないCPUにおいて秘密プログラムを実行することによって実現される。

また、外部メモリ201には、以下に示す処理を経て、図27に示すように、利用履歴データ108およびSAM登録リストが記憶される。

ここで、外部メモリ201のメモリ空間は、SAM105₁の外部（例えば、ホストCPU810）からは見ることはできず、SAM105₁のみが外部メモリ201の記憶領域に対してのアクセスを管理できる。

外部メモリ201としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。

また、スタックメモリ200としては、例えばSARAMが用いられ、図28に示すように、セキュアコンテナ104、コンテンツ鍵データK_C、権利書データ（UCP）106、記憶部192のロック鍵データK_{Loc}、コンテンツプロバイダ101の公開鍵証明書CER_{CP}、利用制御状態データ（UCS）166、およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC_nなどが記憶される。

以下、SAM105₁の機能のうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの各機能ブロックの処理内容を図26を参照しながら説明する。

相互認証部170は、SAM105₁がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ（共有鍵）K_{ss}を生成し、これを暗号化・復号部171に出力する。セッション鍵データK_{ss}は、相互認証を行う度に新たに生成される。

暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービス

センタ102との間で送受信するデータを、相互認証部170が生成したセッション鍵データ K_{ss} を用いて暗号化・復号する。

誤り訂正部181は、セキュアコンテナ104を誤り訂正してダウンロードメモリ管理部182に出力する。

なお、ユーザホームネットワーク103は、セキュアコンテナ104が改竄されているか否かを検出する機能を有していてもよい。

本実施形態では、誤り訂正部181を、SAM105₁に内蔵した場合を例示したが、誤り訂正部181の機能を、例えばホストCPU810などのSAM105₁の外部に持たせてもよい。

ダウンロードメモリ管理部182は、図25に示すようにダウンロードメモリ167が相互認証機能を持つメディアSAM167aを有している場合には、相互認証部170とメディアSAM167aとの間で相互認証を行った後に、誤り訂正後のセキュアコンテナ104を、相互認証によって得られたセッション鍵データ K_{ss} を用いて暗号化して図25に示すダウンロードメモリ167に書き込む。ダウンロードメモリ167としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図29に示すように、HDD(Hard Disk Drive)などの相互認証機能を備えていないメモリをダウンロードメモリ211として用いる場合には、ダウンロードメモリ211内はセキュアではないので、コンテンツファイルCFをダウンロードメモリ211にダウンロードし、機密性の高いキーファイルKFを例えば、図26に示すスタックメモリ200にダウンロードする。

セキュアコンテナ復号部183は、ダウンロードメモリ管理部182から入力したセキュアコンテナ104に格納されたキーファイルKF内のコンテンツ鍵データ K_c 、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC_nを、記憶部192から読み出した対応する期間の配信用鍵データKD₁～KD_nを用いて復号する。

当該復号されたコンテンツ鍵データK_C、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₃は、スタックメモリ200に書き込まれる。

EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

署名処理部189は、記憶部192から読み出したEMDサービスセンタ102の公開鍵データK_{ESC, P}およびコンテンツプロバイダ101の公開鍵データK_{CP, P}を用いて、セキュアコンテナ104内の署名データの検証を行なう。

記憶部192は、SAM105₁の外部から読み出しおよび書き換えできない秘密データとして、図30に示すように、有効期限付きの複数の配信用鍵データKD₁～KD₃、SAM_ID、ユーザID、パスワード、情報参照ID、SAM登録リスト、記録用鍵データK_{STR}、ルートCAの公開鍵データK_{R-CA, P}、EMDサービスセンタ102の公開鍵データK_{ESC, P}、メディア鍵データK_{MED}、EMDサービスセンタ102の公開鍵データK_{ESC, P}、SAM105₁の秘密鍵データK_{SAM1, S}、SAM105₁の公開鍵データK_{SAM1, P}を格納した公開鍵証明書CER_{SAM1}、EMDサービスセンタ102の秘密鍵データK_{ESC, S}を用いた公開鍵証明書CER_{ESC}の署名データSIG₂₂、復号・伸長モジュール163ととの間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアSAMとの間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、並びにメディアSAMの公開鍵証明書データCER_{MEDSAM}（公開鍵暗号化方式を採用した場合）を記憶している。

また、記憶部192には、図26に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部192としては、例えば、フラッシューEEPROM(Electrically Erasable Programmable RAM)が用いられる。

以下、EMDサービスセンタ102から受信した配信用鍵データKD₁～KD

。を記憶部192に格納する際のSAM105₁内での処理の流れを図26を参照しながら説明する。

この場合には、まず、相互認証部170と図23に示す相互認証部150との間で相互認証が行われる。

次に、当該相互認証によって得られたセッション鍵データ K_{ss} で暗号化された3カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD_1,ssc} \sim SIG_{KD_3,ssc}$ が、EMDサービスセンタ102からEMDサービスセンタ管理部185を介してスタックメモリ811に書き込まれる。

次に、暗号化・復号部171において、セッション鍵データ K_{ss} を用いて、配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD_1,ssc} \sim SIG_{KD_3,ssc}$ が復号される。

次に、署名処理部189において、スタックメモリ811に記憶された署名データ $SIG_{KD_1,ssc} \sim SIG_{KD_3,ssc}$ の正当性が確認された後に、配信用鍵データ $KD_1 \sim KD_3$ が記憶部192に書き込まれる。

以下、コンテンツプロバイダ101が提供したセキュアコンテナ104を入力する際のSAM105₁内での処理の流れを図26を参照しながら説明する。

図26に示すSAM105₁の相互認証部170と図3に示す相互認証部120との間で相互認証が行なわれる。

暗号化・復号部171は、当該相互認証によって得られたセッション鍵データ K_{ss} を用いて、コンテンツプロバイダ管理部180を介してコンテンツプロバイダ101から供給されたセキュアコンテナ104を復号する。

次に、署名処理部189は、図5(C)に示す署名データ $SIG_{s,ssc}$ の検証を行なった後に、図5(C)に示す公開鍵証明書データ CER_{cp} 内に格納されたコンテンツプロバイダ101の公開鍵データ $K_{cp,p}$ を用いて、署名データ $SIG_{s,cp}$ 、 $SIG_{t,cp}$ の正当性を検証する。

このとき、署名データ $SIG_{s,cp}$ が正当であると検証されたときに、コンテン

ツファイルCFの作成者および送信者の正当性が確認される。

また、署名データSIG_{7, CP}が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

また、署名処理部189は、記憶部192から読み出した公開鍵データK_{ESC}を用いて、図5(B)に示すキーファイルKF内の署名データSIG_{K1, ESC}の正当性、すなわちキーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102に登録されているか否かの検証を行う。

コンテンツプロバイダ管理部180は、署名データSIG_{S, CP}、SIG_{7, CP}、SIG_{K1, ESC}の正当性が確認されると、セキュアコンテナ104を誤り訂正部181に出力する。

誤り訂正部181は、セキュアコンテナ104を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

ダウンロードメモリ管理部182は、相互認証部170と図25に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104をダウンロードメモリ167に書き込む。

次に、ダウンロードメモリ管理部182は、相互認証部170と図25に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104に格納された図5(B)に示すキーファイルKFをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

そして、セキュアコンテナ復号部183において、記憶部192から入力した対応する期間の配信用鍵データKD₁～KD₃を用いて、図5(B)に示すキーファイルKF内のコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₃が復号される。

そして、復号されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₃がスタックメモリ200に書き込まれる。

以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを利用・購入する処理に関連する各機能ブロックの処理内容を図31を参照しながら説明する。

利用監視部186は、スタックメモリ200から権利書データ106および利用制御状態データ166を読み出し、当該読み出した権利書データ106および利用制御状態データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。

ここで、権利書データ106は、図26を用いて説明したように、復号後にKFに格納されてスタックメモリ200に記憶されている。

また、利用制御状態データ166は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ200に記憶される。

課金処理部187は、図25に示す購入・利用形態決定操作部165からの操作信号S165に応じた利用履歴データ108を作成する。

ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

また、課金処理部187は、必要に応じて、スタックメモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。

ここで、販売価格および標準小売価格データSRPは、復号後にスタックメモリ200に記憶された図5(B)に示すキーファイルKFの権利書データ106内に格納されている。

課金処理部187による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

また、課金処理部187は、操作信号S165に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御状態（UCS: Usage Control Status）データ166を生成し、これをスタックメモリ200に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ166には、コンテンツのID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

なお、決定された購入形態が再生課金である場合には、例えば、SAM105₁からコンテンツプロバイダ101に利用制御状態データ166をコンテンツデータCの購入と同時にリアルタイムに送信し、コンテンツプロバイダ101がEMDサービスセンタ102に、利用履歴データ108を所定の期間内にSAM105₁に取りに行くことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、コンテンツプロバイダ101およびEMDサービスセンタ102の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ166をコンテンツプロバイダ101にリアルタイムに送信する。

EMDサービスセンタ管理部185は、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。

このとき、EMDサービスセンタ管理部185は、署名処理部189において

、秘密鍵データ K_{SAMI} を用いて利用履歴データ108の署名データ $SIG_{200, SAMI}$ を作成し、署名データ $SIG_{200, SAMI}$ を利用履歴データ108と共にEMDサービスセンタ102に送信する。

EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに、当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

ダウンロードメモリ管理部182は、例えば、図25に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツデータC、スタックメモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ198を復号・伸長モジュール管理部184に出力する。

また、復号・伸長モジュール管理部184は、図25に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びにスタックメモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199を復号・伸長モジュール管理部184に出力する。

ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール163がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロック

クとを指定したり、試験時の再生機能を限定したり、試験可能な期間を限定するものなどがある。

以下、SAM105：内での処理の流れについて説明する。

まず、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテナ104の購入形態を決定するまでの処理の流れを図31を参照しながら説明する。

ユーザによる図25に示す購入・利用形態決定操作部165の操作によって、試験モードを示す操作信号S165が課金処理部187に出力されると、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図25に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データK_{ss}による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データK_{ss}による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図25に示す復号部221においてセッション鍵データK_{ss}を用いて復号された後に、復号部222に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデータ199が、図25に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データKcおよび半開示パラメータデータ199に対してセッション鍵データK_{ss}による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長

された後に、電子透かし情報処理部224に出力される。

次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ196がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。

そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

そして、課金処理部187において、決定された購入形態に応じた利用履歴データ108および利用制御状態データ166が生成され、利用履歴データ108が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に、利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

そして、後述する図34（C）に示す新たなキーファイルKF₁が作成され、当該作成されたキーファイルKF₁がダウンロードメモリ管理部182を介してダウンロードメモリ167に記憶される。

図34（C）に示すように、キーファイルKF₁に格納された利用制御状態データ166はストレージ鍵データK_{STR}およびメディア鍵データK_{MED}を用いてDESのCBCモードを利用して順に暗号化されている。

ここで、記録用鍵データK_{STR}は、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。また、メディア鍵データK_{MED}は、記録媒体にユニークなデータである。

また、署名処理部189において、SAM1051の秘密鍵データ $K_{SAM1.0}$ を用いて、キーファイル KF_1 のハッシュ値 H_{K1} が作成され、当該作成されたハッシュ値 H_{K1} が、キーファイル KF_1 と対応付けられてスタックメモリ200に書き込まれる。ハッシュ値 H_{K1} は、キーファイル KF_1 の作成者の正当性およびキーファイル KF_1 が改竄されたか否かを検証するために用いられる。

次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図31を参照しながら説明する。

この場合には、利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、図31に示す復号・伸長モジュール163に出力される。このとき、図31に示す相互認証部170と、図25に示す復号・伸長モジュール163の相互認証部220との間で相互認証が行われる。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcが復号・伸長モジュール163に出力される。

そして、復号・伸長モジュール163の復号部222において、コンテンツ鍵データKcを用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。

このとき、課金処理部187によって、操作信号S165に応じて、外部メモリ201に記憶されている利用履歴データ108が更新される。

利用履歴データ108は、外部メモリ201から読み出された後、相互認証を経て、EMDサービスセンタ管理部185を介して、署名データSIG200、SAM1と共にEMDサービスセンタ102に送信される。

次に、図32に示すように、例えば、前述したようにネットワーク機器1601のダウンロードメモリ167にダウンロードされたコンテンツファイルCFの

購入形態を決定した後に、当該コンテンツファイルCFを格納した新たなセキュアコンテナ104xを生成し、パス191を介して、AV機器160₂のSAM105₂にセキュアコンテナ104xを転送する場合のSAM105₁内での処理の流れを図33を参照しながら説明する。

ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器160₂に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部187に出力される。

これにより、課金処理部187は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ108を更新する。

また、課金処理部187は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態を示す利用制御状態データ166をEMDサービスセンタ管理部185を介してEMDサービスセンタ102に送信する。

また、ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図5(A)に示すコンテンツファイルCFおよびその署名データSIG_{1,CF}と、キーファイルKFおよびその署名データSIG_{1,KF}と、キーファイルKF₁およびそのハッシュ値H_{K1}とをSAM管理部190に出力する。このとき、SAM105₁の相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号が行われる。

また、署名処理部189は、コンテンツファイルCFのハッシュ値をとり、秘密鍵データK_{SAM1,S}を用いて署名データSIG_{41,SAM1}を作成し、これをSAM管理部190に出力する。

また、署名処理部189は、キーファイルKF₁のハッシュ値をとり、秘密鍵データK_{SAM1,S}を用いて署名データSIG_{42,SAM1}を作成し、これをSAM管理部190に出力する。

また、SAM管理部190は、記憶部192から、図34(D)に示す公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}と、公開鍵証明書デー

タCER_{SAM1}およびその署名データSIG_{22, SSC}とを読み出す。

また、相互認証部170は、SAM105₂との間で相互認証を行って得たセッション鍵データK_{SS}を暗号化・復号部171に出力する。

SAM管理部190は、図34(A), (B), (C), (D)に示すデータからなる新たなセキュアコンテナ104xを生成し、暗号化・復号部171において、セッション鍵データK_{SS}を用いてセキュアコンテナ104xを暗号化した後に、図32に示すAV機器160₂のSAM105₂に出力する。

このとき、SAM105₁とSAM105₂との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

以下、図32に示すように、SAM105₁から入力したセキュアコンテナ104xを、RAM型などの記録媒体(メディア)130₄に書き込む際のSAM105₂内での処理の流れを、図35を参照しながら説明する。

ここで、RAM型の記録媒体130₄は、例えば、セキュアでないRAM領域134、メディアSAM133およびセキュアRAM領域132を有している。

この場合には、SAM105₂のSAM管理部190は、図32および図35に示すように、ネットワーク機器160₁のSAM105₁からセキュアコンテナ104xを入力する。

そして、暗号化・復号部171において、SAM管理部190を介して入力したセキュアコンテナ104xが、相互認証部170とSAM105₁の相互認証部170との間の相互認証によって得られたセッション鍵データK_{SS}を用いて復号される。

次に、署名処理部189において、公開鍵データK_{CP, P}を用いて、署名データSIG_{6, CP}の正当性が検証され、コンテンツファイルCFの作成者の正当性が確認される。また、署名処理部189において、公開鍵データK_{SAM1, P}を用いて、署名データSIG_{41, SAM1}の正当性が検証され、コンテンツファイルCFの送信

者の正当性が確認される。

そして、コンテンツファイルCFの作成者および送信者が正当であると確認された後に、SAM管理部190から記録モジュール管理部855にコンテンツファイルCFが出力され、コンテンツファイルCFが図32に示すRAM型の記録媒体1304のRAM領域134に書き込まれる。

また、セッション鍵データ K_{SES} を用いて復号されたキーファイルKFおよびその署名データ $SIG_{7,CP}$ 、 $SIG_{42,SAM1}$ と、キーファイルKF₁およびそのハッシュ値 H_{K1} と、公開鍵署名データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22,ESC}$ とが、スタックメモリ200に書き込まれる。

次に、署名処理部189は、スタックメモリ200から読み出した署名データ $SIG_{22,ESC}$ を、記憶部192から読み出した公開鍵データ $K_{ESC,P}$ を用いて検証して、公開鍵証明書データ CER_{SAM1} の正当性を確認する。

そして、署名処理部189は、公開鍵証明書データ CER_{SAM1} の正当性を確認すると、公開鍵証明書データ CER_{SAM1} に格納された公開鍵データ $K_{SAM1,P}$ を用いて、スタックメモリ200に記憶されている署名データ $SIG_{42,SAM1}$ の正当性を検証する。そして、署名データ $SIG_{42,SAM1}$ が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

また、署名処理部189は、スタックメモリ200から読み出した署名データ $SIG_{1,ESC}$ を、記憶部192から読み出した公開鍵データ $K_{ESC,P}$ を用いて検証して、公開鍵証明書データ CER_{CP} の正当性を確認する。

そして、署名処理部189は、公開鍵証明書データ CER_{CP} の正当性を確認すると、公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP,P}$ を用いて、スタックメモリ200に記憶されている署名データ $SIG_{7,SAM1}$ の正当性を検証する。そして、署名データ $SIG_{7,SAM1}$ が正当であると検証されたときに、キーファイルKFの作成者の正当性が確認される。

キーファイルKFの作成者および送信者が正当であることが確認されると、キーファイルKFがスタックメモリ200から読み出され、記録モジュール管理部855を介して、図34に示すRAM型の記録媒体130₄のセキュアRAM領域132に書き込まれる。

また、署名処理部189は、公開鍵データ $K_{SAM, P}$ を用いて、ハッシュ値 H_{K1} の正当性を検証し、キーファイルKF₁の作成者および送信者の正当性を確認する。

そして、キーファイルKF₁の作成者および送信者の正当性が確認されると、図34(C)に示すキーファイルKF₁をスタックメモリ200から読み出して暗号化・復号部173に出力する。

なお、当該例では、キーファイルKF₁の作成者と送信元とが同じ場合を述べたが、キーファイルKF₁の作成者と送信元とが異なる場合には、キーファイルKF₁に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

そして、暗号化・復号部173は、記憶部192から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を順に用いてキーファイルKF₁内のコンテンツ鍵データKcおよび利用制御状態データ166を暗号化して記録モジュール管理部855に出力する。

そして、記録モジュール管理部855によって、暗号化されたキーファイルKF₁が、RAM型の記録媒体130₄のセキュアRAM領域132に記録される。

なお、メディア鍵データ K_{MED} は、図33に示す相互認証部170と図32に示すRAM型の記録媒体130₄のメディアSAM133との間の相互認証によって記憶部192に事前に記憶されている。

ここで、記録用鍵データ K_{STR} は、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc

）機器などの種類（当該例では、AV機器160₂）に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。なお、SACDとDVDとでは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データK_{STR}は、このような場合において、不正コピーを防止する役割を果たす。

なお、本実施形態では、記録用鍵データK_{STR}を用いた暗号化を行わないようにしてもよい。

また、メディア鍵データK_{MED}は、記録媒体（当該例では、RAM型の記録媒体130₄）にユニークなデータである。

メディア鍵データK_{MED}は、記録媒体（当該例では、図32に示すRAM型の記録媒体130₄）側に格納されており、記録媒体のメディアSAMにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データK_{MED}は、記録媒体にメディアSAMが搭載されている場合には、当該メディアSAM内に記憶されており、記録媒体にメディアSAMが搭載されていない場合には、例えば、RAM領域内のホストCPU810の管理外の領域に記憶されている。

なお、本実施形態のように、機器側のSAM（当該例では、SAM105₂）とメディアSAM（当該例では、メディアSAM133）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データK_{MED}を機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

また、購入者鍵データK_{PIN}は、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユー

ザに対してEMDサービスセンタ102によって割り当てられる。購入者鍵データ K_{PIN} は、EMDサービスセンタ102において管理される。

また、上述した実施形態では、記録モジュール260を用いて、キーファイル KF 、 KF_1 をRAM型の記録媒体130₁のセキュアRAM領域132に記録する場合を例示したが、図32において点線で示すように、SAM105₂からメディアSAM133にキーファイル KF 、 KF_1 を記録するようにしてもよい。

次に、コンテンツの購入形態が未決定の図12に示すROM型の記録媒体130₁をユーザホームネットワーク303がオフラインで配給を受けた場合に、AV機器160₂において購入形態を決定する際の処理の流れを図36および図37を参照しながら説明する。

AV機器160₂のSAM105₂は、まず、図37に示す相互認証部170と図12に示すROM型の記録媒体130₁のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データ K_{MED} を入力する。

なお、SAM105₂が、事前にメディア鍵データ K_{MED} を保持している場合には、当該入力を行わなくても良い。

次に、ROM型の記録媒体130₁のセキュアRAM領域132に記録されているセキュアコンテナ104に格納された図5(B)、(C)に示すキーファイル KF およびその署名データ $SIG_{T,CP}$ と、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{I,ESC}$ とを、メディアSAM管理部197あるいは図示しない読み出しモジュール管理部を介して入力し、これをスタックメモリ200に書き込む。

次に、署名処理部189において、署名データ $SIG_{I,ESC}$ の正当性を確認した後に、公開鍵証明書データ CER_{CP} から公開鍵データ $K_{CP,P}$ を取り出し、この公開鍵データ $K_{CP,P}$ を用いて、署名データ $SIG_{T,CP}$ の正当性、すなわちキー

ファイルKFの送信者の正当性を検証する。

また、署名処理部189において、記憶部192から読み出した公開鍵データK_{Esc.P}を用いて、キーファイルKFに格納された署名データSIG_{K1.Esc}の正当性、すなわちキーファイルKFの作成者の正当性を検証する。

署名処理部189において署名データSIG_{7.CP}、SIG_{K1.Esc}の正当性が確認されると、スタックメモリ200からセキュアコンテナ復号部183に、キーファイルKFを読み出す。

次に、セキュアコンテナ復号部183において、対応する期間の配信用鍵データKD₁～KD₇を用いて、キーファイルKFに格納されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₇が復号され、これらがスタックメモリ200に書き込まれる。

次に、図37に示す相互認証部170と図36に示す復号・伸長モジュール163との間で相互認証を行った後に、SAM105₂の復号・伸長モジュール管理部184は、スタックメモリ200に記憶されているコンテンツ鍵データKcおよび権利書データ106に格納された半開示パラメータデータ199、並びにROM型の記録媒体130₁のROM領域131から読み出したコンテンツファイルCFに格納されたコンテンツデータCを図36に示す復号・伸長モジュール163に出力する。次に、復号・伸長モジュール163において、コンテンツデータCがコンテンツ鍵データKcを用いて半開示モードで復号された後に伸長され、再生モジュール270に出力される。そして、再生モジュール270において、復号・伸長モジュール163からのコンテンツデータCが再生される。

次に、ユーザによる図36に示す購入形態決定操作部165の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号S165が課金処理部187に入力される。

次に、課金処理部187は、操作信号S165に応じた利用制御状態データ1

66を作成し、これをスタックメモリ200に書き込む。

次に、スタックメモリ200から暗号化・復号部173に、コンテンツ鍵データKcおよび利用制御状態データ166が出力される。

次に、暗号化・復号部173は、スタックメモリ200から入力したコンテンツ鍵データKcおよび利用制御状態データ166を、記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{FIN}を用いて順次に暗号化してスタックメモリ200に書き込む。

次に、メディアSAM管理部197において、スタックメモリ200から読み出した、暗号化されたコンテンツ鍵データKcおよび利用制御状態データ166と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃を用いて図34(C)に示すキーファイルKF₁が生成される。

また、署名処理部189において、図34(C)に示すキーファイルKF₁のハッシュ値H_{K1}が生成され、当該ハッシュ値H_{K1}がメディアSAM管理部197に出力される。

次に、図37に示す相互認証部170と図36に示すメディアSAM133との間で相互認証を行った後に、メディアSAM管理部197は、キーファイルKF₁およびハッシュ値H_{K1}を、図36に示す記録モジュール271を介してROM型の記録媒体130₁のセキュアRAM領域132に書き込む。

これにより、購入形態が決定されたROM型の記録媒体130₁が得られる。

このとき、課金処理部187が生成した利用制御状態データ166および履歴データ108は、所定のタイミングで、スタックメモリ200および外部メモリ201からそれぞれ読み出しされたEMDサービスセンタ102に送信される。

なお、ROM型の記録媒体130₁のメディアSAM133にキーファイルKFが格納されている場合には、図36において点線で示されるように、SAM1

05₂はメディアSAM133からキーファイルKFを入力する。また、この場合に、SAM105₂は、作成したキーファイルKF₁をメディアSAM133に書き込む。

以下、図38に示すように、AV機器160₁において購入形態が未決定のROM型の記録媒体130₁からセキュアコンテナ104を読み出して新たなセキュアコンテナ104_yを生成し、これをAV機器160₂に転送し、AV機器160₂において購入形態を決定してRAM型の記録媒体130₂に書き込む際の処理の流れを図39、図40を参照しながら説明する。

なお、ROM型の記録媒体130₁からRAM型の記録媒体130₂へのセキュアコンテナ104の転送は、図1に示すネットワーク機器160₁およびAV機器160₁～160₄のいずれの間で行ってもよい。

まず、AV機器160₁のSAM105₁とROM型の記録媒体130₁のメディアSAM133との間で相互認証を行い、ROM型の記録媒体130₁のメディア鍵データK_{MED1}をSAM105₁に転送する。

また、AV機器160₂のSAM105₂とRAM型の記録媒体130₂のメディアSAM133との間で相互認証を行い、RAM型の記録媒体130₂メディア鍵データK_{MED2}をSAM105₂に転送する。

なお、メディア鍵データK_{MED1}、K_{MED2}を用いた暗号化をメディアSAM133およびメディアSAM133において行う場合には、メディア鍵データK_{MED1}、K_{MED2}の転送は行わない。

次に、SAM105₂は、図39に示すように、メディアSAM管理部197あるいは図示しない読み出しモジュール管理部を介して、ROM型の記録媒体130₁のROM領域131から読み出した図5(A)に示すコンテンツファイルCFおよびその署名データSIG_{cf}と、セキュアRAM領域132から読み出した図5(B)、(C)に示すキーファイルKFおよびその署名データSIG_kと、公開鍵証明書データCER_{cf}およびその署名データSIG_{1_esc}とを、暗

号化・復号部171に出力する。

また、メディアSAM管理部197から署名処理部189に、コンテンツファイルCFおよびキーファイルKFが出力される。

そして、署名処理部189において、コンテンツファイルCFおよびキーファイルKFのハッシュ値がとられ、秘密鍵データ K_{SAMs} を用いて、それぞれ署名データ $SIG_{sso, SAMs}$ 、 $SIG_{ssi, SAMs}$ が生成され、これらが暗号化・復号部171に出力される。

また、公開鍵証明書データ CER_{SAMs} およびその署名データ $SIG_{ssi, ESc}$ が記憶部192から読み出されて暗号化・復号部171に出力される。

そして、図40に示すセキュアコンテナ104yが、暗号化・復号部171においてSAM105₂と105₂との間の相互認証によって得られたセッション鍵データ K_{ss} を用いて暗号化された後に、SAM管理部190を介して、AV機器160₂のSAM105₂に出力される。

SAM105₂では、図41に示すように、SAM管理部190を介してSAM105₂から入力した図40に示すセキュアコンテナ104yを暗号化・復号部171においてセッション鍵データ K_{ss} を用いて復号した後に、セキュアコンテナ104y内に格納された署名データ $SIG_{s, CP}$ 、 $SIG_{sso, SAMs}$ の正当性、すなわちコンテンツファイルCFの作成者および送信者の正当性を確認する。

そして、コンテンツファイルCFの作成者および送信者が正当であると確認された後に、メディアSAM管理部197を介してRAM型の記録媒体130₂のRAM領域134にコンテンツファイルCFが書き込まれる。

また、SAM管理部190を介してSAM105₂から入力されたキーファイルKFおよびその署名データ $SIG_{t, CP}$ 、 $SIG_{sso, SAMs}$ と、公開鍵証明書データ CER_{SAMs} およびその署名データ $SIG_{ssi, ESc}$ とが、スタックメモリ200に書き込まれた後に、暗号化・復号部171においてセッション鍵データ K_{ss}

を用いて復号される。

次に、当該復号された署名データSIG_{ssl, enc}が、署名処理部189において署名検証され、公開鍵証明書データCERT_{sam}の正当性が確認されると、公開鍵証明書データCERT_{sam}に格納された公開鍵データK_{sam}を用いて、署名データSIG_{7, cp}、SIG_{ssl, sam}の正当性、すなわちキーファイルKFの作成者および送信者の正当性が確認される。

そして、キーファイルKFの作成者および送信者の正当性が確認されると、スタックメモリ200からキーファイルKFが読み出されてセキュアコンテナ復号部183に出力される。

次に、セキュアコンテナ復号部183は、対応する期間の配信用鍵データKD₁～KD₉を用いて、キーファイルKFを復号し、当該復号したキーファイルKFをスタックメモリ200に書き込む。

次に、スタックメモリ200に記憶されている既に復号されたキーファイルKFに格納された権利書データ106が、利用監視部186に出力される。利用監視部186は、権利書データ106に基づいて、コンテンツの購入形態および利用形態が管理される。

次に、例えば、ユーザによって試験モードが選択されると、既にセッション鍵データK_{ss}で復号されたコンテンツファイルCFのコンテンツデータCと、スタックメモリ200に記憶されたコンテンツ鍵データK_c、権利書データ106から得られた半開示パラメータデータ199およびユーザ電子透かし情報用データ196とが、相互認証を経た後に、図38に示す復号・伸長モジュール管理部184を介して再生モジュール270に出力される。そして、再生モジュール270において、試験モードに対応したコンテンツデータCの再生が行われる。

次に、ユーザによる図38に示す購入・利用形態決定操作部165の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号S165が、課金処理部187に出力される。

そして、課金処理部187において、決定された購入・利用形態に応じて利用制御状態データ166および利用履歴データ108が生成され、これがスタックメモリ200および外部メモリ201にそれぞれ書き込まれる。

次に、コンテンツ鍵データK_Cおよび利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MEDIA}および購入者鍵データK_{PIR}を用いて順に暗号化され、記録モジュール管理部855に出力される。そして、例えば、記録モジュール管理部855において、図34(C)に示すキーファイルKF₁が作成され、キーファイルKF₁がメディアSAM管理部197を介してRAM型の記録媒体130₅のメディアSAM133に書き込まれる。

また、セキュアコンテナ104_yに格納されたコンテンツファイルCFは、記録モジュール管理部855によって、RAM型の記録媒体130₅のRAM領域134に書き込まれる。

また、利用制御状態データ166および利用履歴データ108は、所定のタイミングで、EMDサービスセンタ102に送信される。

以下、SAM105₁～105₄の実現方法について説明する。

SAM105₁～105₄の機能をハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図26に示す各機能を実現するためのセキュリティ機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

例えば、図26に示す暗号化・復号部171などのモジュールは、例えば、処

理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。

また、図26に示す記憶部192や、図26に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ（フラッシュROM）が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM105、～105₄に内蔵されるメモリとして、強誘電体メモリ（FeRAM）を用いてもよい。

また、SAM105、～105₄には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

上述したように、SAM105、～105₄は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM105、～105₄を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリー空間を管理するMMU(Memory Management Unit)を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。

また、SAM105、～105₄は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウェアICE、ソフトウェアICE）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。

SAM105₁～105₄。自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

SAM105₁～105₄の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理をおこなう場合と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（Mini OS）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

次に、図25に示す復号・伸長モジュール163について説明する。

図25に示すように、復号・伸長モジュール163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。

相互認証部220は、復号・伸長モジュール163がSAM105₁からデータを入力する際に、図32に示す相互認証部170との間で相互認証を行ってセッション鍵データK_{ss}を生成する。

復号部221は、SAM105₁から入力したコンテンツ鍵データK_c、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテ

ンツデータCを、セッション鍵データK_{ss}を用いて復号する。そして、復号部221は、復号したコンテンツ鍵データK_cおよびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データK_cを用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。

伸長部223は、例えば、図5(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRA C3方式で伸長処理を行う。

電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータCを再生モジュール169に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータCを再生するときに、復号・伸長モジュール163において埋め込まれる。

なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを復号部222に指示する。

また、半開示処理部225は、その他に、半開示パラメータデータ199に基づいて、試験時の再生機能を限定したり、試験可能な期間を限定するなどの制御

を行う。

再生モジュール169は、復号および伸長されたコンテンツデータCに応じた再生を行う。

次に、コンテンツプロバイダ101、EMDサービスセンタ102およびユーザホームネットワーク103の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。

図42(A)は、コンテンツプロバイダ101からSAM105₁にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からSAM105₁に、コンテンツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データK_{ss}で暗号化したモジュールMod_sが送信される。

モジュールMod_sには、モジュールMod_sおよびその秘密鍵データK_{cr,s}による署名データSIG_{cr}が格納されている。

モジュールMod_sには、コンテンツプロバイダ101の秘密鍵データK_{cr,p}を格納した公開鍵証明書データCER_{cr}と、公開鍵証明書データCER_{cr}に対しての秘密鍵データK_{ss,cr}による署名データSIG_{ss,cr}と、送信するデータDataとが格納されている。

このように、公開鍵証明書データCER_{cr}を格納したモジュールMod_sを、コンテンツプロバイダ101からSAM105₁に送信することで、SAM105₁において署名データSIG_{cr}の検証を行なう際に、EMDサービスセンタ102からSAM105₁に公開鍵証明書データCER_{cr}を送信する必要がなくなる。

図42(B),(C)は、コンテンツプロバイダ101からSAM105₁にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマット

トを説明するための図である。

この場合には、コンテンツプロバイダ101からSAM105₁に、コンテンツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データK_{ss}で暗号化した図42(B)に示すモジュールMod_{s2}が送信される。

モジュールMod_{s2}には、送信するデータDataと、その秘密鍵データK_{cr,s}による署名データSIG_{cr}とが格納されている。

また、EMDサービスセンタ102からSAM105₁には、EMDサービスセンタ102とSAM105₁との間の相互認証によって得たセッション鍵データK_{ss}で暗号化した図42(C)に示すモジュールMod_{s3}が送信される。

モジュールMod_{s3}には、コンテンツプロバイダ101の公開鍵証明書データCER_{cr}と、その秘密鍵データK_{esc,s}による署名データSIG_{esc}とが格納されている。

図42(D)は、SAM105₁からコンテンツプロバイダ101にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データK_{ss}で暗号化したモジュールMod_{s4}が送信される。

モジュールMod_{s4}には、モジュールMod_{s3}およびその秘密鍵データK_{sam1,s}による署名データSIG_{sam1}が格納されている。

モジュールMod_{s5}には、SAM105₁の秘密鍵データK_{sam1,p}を格納した公開鍵証明書データCER_{sam1}と、公開鍵証明書データCER_{sam1}に対しての秘密鍵データK_{esc,s}による署名データSIG_{esc}と、送信するデータDataとが格納されている。

このように、公開鍵証明書データCER_{sam1}を格納したモジュールMod_{s5}を

、SAM105₁ からコンテンツプロバイダ101に送信することで、コンテンツプロバイダ101において署名データSIG_{SAM1}の検証を行なう際に、EMDサービスセンタ102からコンテンツプロバイダ101に公開鍵証明書データCER_{SAM1}を送信する必要がなくなる。

図42(E)、(F)は、SAM105₁ からコンテンツプロバイダ101にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁ からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM105₁ との間の相互認証によって得たセッション鍵データK_{ss}で暗号化した図42(E)に示すモジュールMod_{ss}が送信される。

モジュールMod_{ss}には、送信するデータDataと、その秘密鍵データK_{sa}_{m1}による署名データSIG_{SAM1}とが格納されている。

また、EMDサービスセンタ102からコンテンツプロバイダ101には、EMDサービスセンタ102とコンテンツプロバイダ101との間の相互認証によって得たセッション鍵データK_{ss}で暗号化した図42(F)に示すモジュールMod_{sy}が送信される。

モジュールMod_{sy}には、SAM105₁ の公開鍵証明書データCER_{SAM1}と、その秘密鍵データK_{sc}による署名データSIG_{sc}とが格納されている。

図43(G)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データK_{ss}で暗号化したモジュールMod_{ss}が送信される。

モジュールMod_sには、モジュールMod_sおよびその秘密鍵データK_{cp,s}による署名データSIG_{cp}が格納されている。

モジュールMod_sには、コンテンツプロバイダ101の秘密鍵データK_{cp,r}を格納した公開鍵証明書データCER_{cp}と、公開鍵証明書データCER_{cp}に対しての秘密鍵データK_{esc,s}による署名データSIG_{esc}と、送信するデータDataとが格納されている。

図43(H)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データK_{ss}で暗号化した図43(H)に示すモジュールMod_sが送信される。

モジュールMod_sには、送信するデータDataと、その秘密鍵データK_{cp,s}による署名データSIG_{cp}とが格納されている。

このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公開鍵証明書データCER_{cp}は既に登録されている。

図43(I)は、SAM105₁からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁からEMDサービスセンタ102に、EMDサービスセンタ102とSAM105₁との間の相互認証によって得たセッション鍵データK_{ss}で暗号化したモジュールMod_{s1}が送信される。

モジュールMod_{s1}には、モジュールMod_{s2}およびその秘密鍵データK_{sam1,s}による署名データSIG_{sam1}が格納されている。

モジュールMod_{s2}には、SAM105₁の秘密鍵データK_{sam1,r}を格納した

公開鍵証明書データ CER_{SAM1} と、公開鍵証明書データ CER_{SAM1} に対しての秘密鍵データ $K_{Esc,s}$ による署名データ SIG_{Esc} と、送信するデータ $Data$ とが格納されている。

図 43 (J) は、 $SAM105_1$ から EMD サービスセンタ 102 にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ から EMD サービスセンタ 102 に、EMD サービスセンタ 102 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{ss} で暗号化した図 43 (J) に示すモジュール Mod_{ss} が送信される。

モジュール Mod_{ss} には、送信するデータ $Data$ と、その秘密鍵データ $K_{SA_{MI,s}}$ による署名データ SIG_{SAM1} とが格納されている。

このとき、EMD サービスセンタ 102 には $SAM105_1$ の公開鍵証明書データ CER_{SAM1} は既に登録されている。

以下、 $SAM105_1 \sim 105_4$ の出荷時における EMD サービスセンタ 102 への登録処理について説明する。

なお、 $SAM105_1 \sim 105_4$ の登録処理は同じであるため、以下、 $SAM105_1$ の登録処理について述べる。

$SAM105_1$ の出荷時には、図 24 に示す EMD サービスセンタ 102 のサーバ 141 によって、SAM 管理部 149 を介して、図 26 などに示す記憶部 192 に以下に示す鍵データが初期登録される。

また、 $SAM105_1$ には、例えば、出荷時に、記憶部 192 などに、 $SAM105_1$ が EMD サービスセンタ 102 に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部 192 には、例えば、図 30 において左側に「*」が付されている $SAM105_1$ の識別子 SAM_ID 、記録用鍵データ K_{STR} 、ルート認

を格納したコンテンツファイルとを含むモジュールを受け、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信する。

また、本発明の第３６の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

本発明の第３６の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号され権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

本発明の第３７の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

本発明の第３７の観点のデータ提供システムの作用は以下に示すようになる。
。 前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

また、本発明の第38の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

以下、本発明の第38の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。

当該作成されたキーファイルは、前記管理装置から前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは

記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

また、本発明の第 3 9 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

以下、本発明の第 3 9 の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格

納された前記コンテンツ鍵データおよび前記権利書データが復号し、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

また、本発明の第40の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

以下、本発明の第40の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱

いが決定される。

また、本発明の第41の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

以下、本発明の第41の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該作成されたキーファイルが前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

また、本発明の第42の観点のデータ提供システムは、データ提供装置からデ

ータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

以下、本発明の第42の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に配給される。

そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

データ提供システム。

また、本発明の第43の観点のデータ提供システムは、データ提供装置からデ

ータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

以下、本発明の第43の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

また、本発明の第44の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給

装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

以下、本発明の第44の観点のデータ提供システムの作用を説明する。

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールが、例えば、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して提供される。

次に、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納した第1のモジュールおよび第2のモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納することで、データ処理装置において、データ提供装置の関係者が作成した権利書データ

に基づいたコンテンツデータの取り扱い（利用）を行わせることが可能になる。

また、前記第 2 のモジュールは、所定の通信プロトコルに依存しない形式で前記データ配給装置から前記データ処理装置に配給されることから、前記第 2 のモジュールに格納されるコンテンツデータの圧縮方式や暗号化方式などを前記データ提供装置が任意に決定できる。

本発明の第 4 5 の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

以下、本発明の第 4 5 の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵データをを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールが提供される。

そして、前記データ配給装置から前記データ処理装置に、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いが決定される。

また、本発明の第46の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を

受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第 4 7 の観点のデータ提供システムは、データ提供装置から第 1 のデータ配給装置および第 2 のデータ配給装置にコンテンツデータを提供し、前記第 1 のデータ配給装置および前記第 2 のデータ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記第 1 のデータ配給装置、前記第 2 のデータ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記第 1 のデータ配給装置および前記第 2 のデータ配給装置に提供し、前記第 1 のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを前記データ処理装置に配給し、前記第 2 のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 3 のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第 2 のモジュールおよび前記第 3 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第 4 8 の観点のデータ提供システムは、第 1 のデータ提供装置からデータ配給装置に第 1 のコンテンツデータを提供し、第 2 のデータ提供装置からデータ配給装置に第 2 のコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記第 1 のデータ提供装置、前記第 2 のデータ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化さ

れた第1のコンテンツ鍵データと前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のキーファイルと、暗号化された第2のコンテンツ鍵データと前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のキーファイルとを作成し、前記第1のデータ提供装置は、前記第1のコンテンツ鍵データを用いて暗号化された前記第1のコンテンツデータを格納した第1のコンテンツファイルと、前記管理装置から受けた前記第1のキーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記第2のデータ提供装置は、前記第2のコンテンツ鍵データを用いて暗号化された前記第2のコンテンツデータを格納した第2のコンテンツファイルと、前記管理装置から受けた前記第2のキーファイルとを格納した第2のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のコンテンツファイル、前記第1のキーファイル、前記第2のコンテンツファイルおよび前記第2のキーファイルを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データ、前記第2のコンテンツ鍵データ、前記第1の権利書データおよび前記第2の権利書データを復号し、当該復号した第1の権利書データに基づいて前記第1のコンテンツデータの取り扱いを決定し、前記復号した第2の権利書データに基づいて前記第2のコンテンツデータの取り扱いを決定する。

また、本発明の第49の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテ

ンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第50の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第51の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであっ

て、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第52の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第53の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第54の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録し

て個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第55の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第56の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記

データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第56の観点のデータ提供システムは、好ましくは、前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する。

また、本発明の第56の観点のデータ提供システムは、好ましくは、前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する。

また、本発明の第57の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格

納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第58の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第59の観点のデータ提供システムは、データ提供装置、デー

タ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルを格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第60の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給

を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 6 1 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 6 2 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第63の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第64の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を

有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルを格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第65の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は

、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第66の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第67の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスソースに対応する前記管理装置に提供し、当該管理装置から受けたコン

テンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第68の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスタソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ

処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第69の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る。

また、本発明の第70の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであっ

て、前記データ提供装置は、コンテンツデータを提供し、前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する。

また、本発明の第34の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第35の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテン

鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第36の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第37の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ

鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第38の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第39の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提

供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第40の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第41の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プ

ロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第42の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第43の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書デ

ータを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第44の観点のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第45の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを、前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュール

ルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第46の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第47の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ配給装置に配給し、前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第48の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイル

に格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第49の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第50の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテ

ンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第 5 1 の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第 5 2 の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データ

および前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第53の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第54の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用

いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第55の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテ

ンツデータの取り扱いを決定する。

また、本発明の第56の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第57の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当

該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第58の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第59の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツ

データの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第60の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第61の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用い

てコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第62の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ

処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第63の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第64の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイル

を作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第65の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給

を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第66の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第67の観点のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提

供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る。

また、本発明の第68の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータを提供し、前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する。

また、本発明の第71の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムであって、前記

データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第72の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第73の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記デ

ータ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した複数の第2のモジュールを、前記データ処理装置との間の相互認証によって得られた共有鍵を用いて暗号化した後に、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記複数の第2のモジュールを前記共有鍵を用いて復号し、当該復号した前記複数の第2のモジュールのなかから単数または複数の第2のモジュールを選択し、前記第2のモジュールの配給サービスに対しての課金処理を行う第1の処理回路と、前記選択された前記第2のモジュールを受けて当該第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する耐タンパ性の第2の処理回路とを有する。

図面の簡単な説明

図1は、本発明の第1実施形態のEMDシステムの全体構成図であり、
図2は、本発明のセキュアコンテナの概念を説明するための図であり、
図3は、図1に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのSAMとの間で送受信されるデータに関連するデータの流れを示す図であり、

図4は、図1に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとEMDサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図であり、

図 5 は、図 1 に示すコンテンツプロバイダから S A M に送信されるセキュアコンテナのフォーマットを説明するための図であり、

図 6 は、図 5 に示すコンテンツファイルに含まれるデータを詳細に説明するための図であり、

図 7 は、図 5 に示すキーファイルに含まれるデータを詳細に説明するための図であり、

図 8 は、コンテンツファイルに格納されるヘッダデータを説明するための図であり、

図 9 は、コンテンツ I D を説明するための図であり、

図 1 0 は、セキュアコンテナのディレクトリ構造を説明するための図であり、

図 1 1 は、セキュアコンテナのハイパーリンク構造を説明するための図であり、

図 1 2 は、本実施形態で用いられる R O M 型の記録媒体の第 1 の例を説明するための図であり、

図 1 3 は、本実施形態で用いられる R O M 型の記録媒体の第 2 の例を説明するための図であり、

図 1 4 は、本実施形態で用いられる R O M 型の記録媒体の第 3 の例を説明するための図であり、

図 1 5 は、本実施形態で用いられる R A M 型の記録媒体の第 1 の例を説明するための図であり、

図 1 6 は、本実施形態で用いられる R A M 型の記録媒体の第 2 の例を説明するための図であり、

図 1 7 は、本実施形態で用いられる R A M 型の記録媒体の第 3 の例を説明するための図であり、

図 1 8 は、コンテンツプロバイダから E M D サービスセンタに送信される登録

要求用モジュールを説明するための図であり、

図 19 は、コンテンツプロバイダから EMD サービスセンタへの登録処理の手順を示すフローチャートであり、

図 20 は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートであり、

図 21 は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートであり、

図 22 は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートであり、

図 23 は、図 1 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図であり、

図 24 は、図 1 に示す EMD サービスセンタの機能ブロック図であり、SAM および図 1 に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図であり、

図 25 は、図 1 に示すユーザホームネットワーク内のネットワーク機器の構成図であり、

図 26 は、図 1 に示すユーザホームネットワーク内の SAM の機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテンツを復号するまでのデータの流れを示す図であり、

図 27 は、図 25 に示す外部メモリに記憶されるデータを説明するための図であり、

図 28 は、スタックメモリに記憶されるデータを説明するための図であり、

図 29 は、図 1 に示すユーザホームネットワーク内のネットワーク機器のその他の構成図であり、

図 30 は、図 26 に示す記憶部に記憶されるデータを説明するための図であり

図 3 1 は、図 1 に示すユーザホームネットワーク内の SAM の機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図であり、

図 3 2 は、図 2 5 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV 機器の SAM に転送する場合の転送元の SAM 内での処理の流れを説明するための図であり、

図 3 3 は、図 3 2 に示す場合における転送元の SAM 内でのデータの流れを示す図であり、

図 3 4 は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図であり、

図 3 5 は、図 3 2 に示す場合において、転送先の SAM において、入力したコンテンツファイルなどを、RAM 型あるいは ROM 型の記録媒体（メディア）に書き込む際のデータの流れを示す図であり、

図 3 6、コンテンツの購入形態が未決定の図 7 に示す ROM 型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV 機器において購入形態を決定する際の処理の流れを説明するための図であり、

図 3 7 は、図 3 6 に示す場合において、SAM 内でのデータの流れを示す図であり、

図 3 8 は、ユーザホームネットワーク内の AV 機器において購入形態が未決定の ROM 型の記録媒体からセキュアコンテナを読み出して、これを他の AV 機器に転送して RAM 型の記録媒体に書き込む際の処理の流れを説明するための図であり、

図 3 9 は、図 3 8 に示す場合における転送元の SAM 内でのデータの流れを示す図であり、

図 4 0 は、図 3 8 において、転送元の SAM から転送先の SAM に転送される

セキュアコンテナのフォーマットを説明するための図であり、

図 4 1 は、図 3 8 に示す場合における転送先の SAM 内でのデータの流れを示す図であり、

図 4 2 は、図 1 に示すコンテンツプロバイダ、EMD サービスセンタおよび SAM の相互間で、イン・バント方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図であり、

図 4 3 は、図 1 に示すコンテンツプロバイダ、EMD サービスセンタおよび SAM の相互間で、イン・バント方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図であり、

図 4 4 は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図であり、

図 4 5 は、SAM が作成する SAM 登録リストのデータフォーマットを説明するための図であり、

図 4 6 は、EMD サービスセンタが作成する SAM 登録リストのデータフォーマットを説明するための図であり、

図 4 7 は、図 1 に示すコンテンツプロバイダの全体動作のフローチャートであり、

図 4 8 は、第 1 実施形態の EMD システムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図であり、

図 4 9 は、本発明の第 1 実施形態の第 2 変形例を説明するための図であり、

図 5 0 は、本発明の第 1 実施形態の第 3 変形例を説明するための図であり、

図 5 1 は、本発明の第 1 実施形態の第 4 変形例において第 1 の手法を採用した場合を説明するための図であり、

図 5 2 は、本発明の第 1 実施形態の第 4 変形例において第 2 の手法を採用した場合を説明するための図であり、

図 5 3 は、本発明の第 1 実施形態の第 5 変形例を説明するための図であり、

図 5 4 は、本発明の第 1 実施形態の第 6 変形例の第 1 のパターンを説明するための図であり、

図 5 5 は、本発明の第 1 実施形態の第 6 変形例の第 2 のパターンを説明するための図であり、

図 5 6 は、本発明の第 1 実施形態の第 6 変形例の第 3 のパターンを説明するための図であり、

図 5 7 は、本発明の第 1 実施形態の第 6 変形例の第 4 のパターンを説明するための図であり、

図 5 8 は、本発明の第 1 実施形態の第 6 変形例の第 5 のパターンを説明するための図であり、

図 5 9 は、本発明の第 2 実施形態の EMD システムの全体構成図であり、

図 6 0 は、図 5 9 に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテンツに関するデータの流れを示す図であり、

図 6 1 は、コンテンツプロバイダにおいて行われるセキュアコンテンツの配送処理の手順を示すフローチャートであり、

図 6 2 は、コンテンツプロバイダにおいて行われるセキュアコンテンツの配送処理の手順を示すフローチャートであり、

図 6 3 は、図 5 9 に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図であり、

図 6 4 は、サービスプロバイダにおいて行われるセキュアコンテンツの作成処理の手順を示すフローチャートであり、

図 6 5 は、図 5 9 に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテンツのフォーマットを説明するための図であり、

図 6 6 は、図 6 5 に示すセキュアコンテンツに格納されたコンテンツファイルの送信形態を説明するための図であり、

図 6 7 は、図 6 5 に示すセキュアコンテナに格納されたキーファイルの送信形態を説明するための図であり、

図 6 8 は、図 5 9 に示すサービスプロバイダの機能ブロック図であり、EMD サービスセンタとの間で送受信されるデータの流れを示す図であり、

図 6 9 は、サービスプロバイダから EMD サービスセンタに送信されるブライスタグ登録要求用モジュールのフォーマットを説明するための図であり、

図 7 0 は、図 5 9 に示す EMD サービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図であり、

図 7 1 は、図 5 9 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図であり、

図 7 2 は、図 5 9 に示す EMD サービスセンタの機能ブロック図であり、SAM との間で送受信されるデータに関連するデータの流れを示す図であり、

図 7 3 は、利用履歴データの内容を説明するための図であり、

図 7 4 は、図 5 9 に示すネットワーク機器の構成図であり、

図 7 5 は、図 7 4 に示す CA モジュールの機能ブロック図であり、

図 7 6 は、図 7 4 に示す SAM の機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図であり、

図 7 7 は、図 7 6 に示す記憶部に記憶されるデータを説明するための図であり

図 7 8 は、図 7 4 に示す SAM の機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図であり、

図 7 9 は、SAM におけるセキュアコンテナの購入形態の決定処理の手順を示すフローチャートであり、

図 8 0 は、購入形態が決定された後のキーファイルのフォーマットを説明する

ための図であり、

図 8 1 は、図 7 4 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に入力形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送先のSAM内での処理の流れを説明するための図であり、

図 8 2 は、図 8 1 に示す場合の転送元のSAM内でのデータの流れを示す図であり、

図 8 3 は、図 8 1 に示す場合の転送先のSAM内でのデータの流れを示す図であり、

図 8 4 は、図 5 9 に示すEMDシステムの全体動作のフローチャートであり、

図 8 5 は、図 5 9 に示すEMDシステムの全体動作のフローチャートであり、

図 8 6 は、第 2 実施形態のEMDシステムにおけるサービスプロバイダからユーザホームネットワークへのセキュアコンテンツの配送形態の一例を説明するための図であり、

図 8 7 は、第 2 実施形態のEMDシステムが採用するセキュアコンテンツの配送プロトコルの一例を説明するための図であり、

図 8 8 は、図 8 7 においてユーザホームネットワークからサービスプロバイダ 3 1 0 へのセキュアコンテンツなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 8 9 は、図 8 7 においてコンテンツプロバイダからEMDサービスセンタへのキーファイルなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 0 は、図 8 7 においてサービスプロバイダからEMDサービスセンタへのプライスタグデータ 3 1 2 などを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 1 は、図 8 7 においてユーザホームネットワーク内でセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 2 は、デジタル放送のデータ放送方式に XML / SMIL / BML を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図であり、

図 9 3 は、デジタル放送のデータ放送方式に MHEG を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図であり、

図 9 4 は、インターフェイスのデータ放送方式に XML / SMIL を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図であり、

図 9 5 は、ユーザホームネットワークから EMD サービスセンタに利用履歴データなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 6 は、ユーザホームネットワーク内においてセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 7 は、本発明の第 2 実施形態の第 1 変形例に係わる 2 個のサービスプロバイダを用いた EMD システムの構成図であり、

図 9 8 は、本発明の第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いた EMD システムの構成図であり、

図 9 9 は、本発明の第 2 実施形態の第 3 変形例に係わる EMD システムの構成図であり、

図 1 0 0 は、本発明の第 2 実施形態の第 4 変形例に係わる EMD システムの構成図であり、

図 1 0 1 は、公開鍵証明書データの取得ルートの形態を説明するための図であり、

図102は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図であり、

図103は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図であり、

図104は、SAMの公開鍵証明書データを無効にする場合の処理を説明するための図であり、

図105は、SAMの公開鍵証明書データを無効にする場合のその他の処理を説明するための図であり、

図106は、図47に示すEMDシステムにおいて、EMDサービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図であり、

図107は、図106に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体のEMDサービスセンタ内に設けた場合のEMDシステムの構成図であり、

図108は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のEMDシステムの構成図であり、

図109は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のEMDシステムの構成図であり、

図110は、コンテンツプロバイダが権利管理用クリアリングハウスおよび電子決済用クリアリングハウスの双方の機能をさらに備えている場合のEMDシステムの構成図であり、

図111は、本発明の第2実施形態の第8変形例において、図47に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテンツのフォーマットを説明するための図であり、

図112は、図111に示すコンテンツファイルとキーファイルとの間のディレクトリ構造データによるリンク関係を説明するための図であり、

図 1 1 3 は、コンテンツファイルとキーファイルとの間のディレクトリ構造のその他の例を説明するための図であり、

図 1 1 4 は、本発明の第 2 実施形態の第 8 変形例において、図 4 7 に示すサードプロバイダから SAM に提供されるセキュアコンテナのフォーマットを説明するための図であり、

図 1 1 5 は、コンボジット型のセキュアコンテナのデータフォーマットの第 1 の概念を説明するための図であり、

図 1 1 6 は、コンボジット型のセキュアコンテナのデータフォーマットの第 2 の概念を説明するための図であり、

図 1 1 7 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいて第 1 の手法を採用した場合を説明するための図であり、

図 1 1 8 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいて第 2 の手法を採用した場合を説明するための図であり、

図 1 1 9 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいてファイル形式を採用しない場合のデータフォーマットを説明するための図であり、

図 1 2 0 は、本発明の第 2 実施形態の第 1 0 変形例に係わる EMD システムの構成図であり、

図 1 2 1 は、本発明の第 2 実施形態の第 1 1 変形例の第 1 のパターンに係わる EMD システムの構成図であり、

図 1 2 2 は、本発明の第 2 実施形態の第 1 1 変形例の第 2 のパターンに係わる EMD システムの構成図であり、

図 1 2 3 は、本発明の第 2 実施形態の第 1 1 変形例の第 3 のパターンに係わる EMD システムの構成図であり、

図 1 2 4 は、本発明の第 2 実施形態の第 1 1 変形例の第 4 のパターンに係わる EMD システムの構成図であり、

図125は、本発明の第2実施形態の第11変形例の第5のパターンに係わるEMDシステムの構成図であり、

図126は、本発明の第2実施形態の第9変形例に係わるEMDシステムの構成図であり、

図127は、本発明の第2実施形態におけるセキュアコンテナのファイル包括大小関係を説明するための図であり、

図128は、本発明の第3実施形態のEMDシステムを説明するための図であり、

図129は、図128に示すEMDサービスセンタの機能ブロック図であり、

図130は、本発明の第3実施形態のEMDシステムの変形例を説明するための図であり、

図131は本発明の第4実施形態のEMDシステムを説明するための図であり、

図132は本発明の第4実施形態のEMDシステムの変形例を説明するための図であり、

図133は本発明の第5実施形態のEMDシステムを説明するための図であり、

図134は本発明の第5実施形態のEMDシステムの変形例を説明するための図であり、

図135は本発明の第5実施形態のEMDシステムのその他の変形例を説明するための図であり、

図136は本発明の第6実施形態のEMDシステムを説明するための図であり、

図137は本発明の第6実施形態のEMDシステムの変形例を説明するための図であり、

図 1 3 8 は本発明の第 6 実施形態の EMD システムのその他の変形例を説明するための図であり、

図 1 3 9 は本発明の第 7 実施形態の EMD システムを説明するための図であり、

図 1 4 0 は本発明の第 7 実施形態の EMD システムの変形例を説明するための図であり、

図 1 4 1 は本発明の第 7 実施形態の EMD システムのその他の変形例を説明するための図であり、

図 1 4 2 は本発明の第 8 実施形態の EMD システムを説明するための図であり、

図 1 4 3 は本発明の第 9 実施形態の EMD システムを説明するための図であり、

図 1 4 4 は、コンテンツプロバイダにおいてキーファイルを作成した場合のキーファイルのフォーマットを説明するための図であり、

図 1 4 5 は、従来の EMD システムの構成図である。

発明を実施するための最良の形態

以下、本発明の実施形態に係わる EMD (Electronic Music Distribution: 電子音楽配信) システムについて説明する。

第 1 実施形態

図 1 は、本実施形態の EMD システム 1 0 0 の構成図である。

本実施形態において、ユーザに配信されるコンテンツ (Content) データとは、情報そのものが価値を有するデジタルデータをいい、画像データ、オーディオデータ、プログラム (ソフトウェア) などがあるが、以下、音楽データを例に説明する。

図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ（クリアリング・ハウス、以下、ESCとも記す）102およびユーザホームネットワーク103を有する。

ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM105₁～105₄が、それぞれ請求項1、請求項6、請求項104および請求項109などに係わるデータ提供装置、管理装置およびデータ処理装置に対応している。

先ず、EMDシステム100の概要について説明する。

EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCを暗号化する際に用いたコンテンツ鍵データKc、コンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある権威機関であるEMDサービスセンタ102に送る。

EMDサービスセンタ102は、コンテンツプロバイダ101から受けたコンテンツ鍵データKc、権利書データ106並びに電子透かし情報鍵データを登録（認証および権威化）する。

また、EMDサービスセンタ102は、対応する期間の配信用鍵データKD₁～KD₅で暗号化したコンテンツ鍵データKc、権利書データ106および自らの署名データなどを格納したキーファイルKFを作成し、これをコンテンツプロバイダ101に送る。

ここで、当該署名データは、キーファイルKFの改竄の有無、キーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102において正規に登録されたことを検証するために用いられる。

また、コンテンツプロバイダ101は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成し、当該生成したコンテン

ツファイルCFと、EMDサービスセンタ102から受けたキーファイルKFと、自らの署名データなどを格納したセキュアコンテナ（本発明のモジュール）104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク103に配給する。

ここで、セキュアコンテナ104内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

ユーザホームネットワーク103は、例えば、ネットワーク機器160₁およびAV機器160₂～160₄を有する。

ネットワーク機器160₁は、SAM(Secure Application Module)105₁を内蔵している。

AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。SAM105₁～105₄相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルインタフェースバスなどのバス191を介して接続されている。

SAM105₁～105₄は、ネットワーク機器160₁がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および／または、コンテンツプロバイダ101からAV機器160₂～160₄に記録媒体を介してオフラインで供給されたセキュアコンテナ104に対応する期間の配信用鍵データKD₁～KD₃を用いて復号した後に、署名データの検証を行う。

SAM105₁～105₄に供給されたセキュアコンテナ104は、ネットワーク機器160₁およびAV機器160₂～160₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

を格納したコンテンツファイルとを含むモジュールを受け、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信する。

また、本発明の第３６の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

本発明の第３６の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号され権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

本発明の第３７の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

本発明の第３７の観点のデータ提供システムの作用は以下に示すようになる。
。 前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

また、本発明の第38の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

以下、本発明の第38の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。

当該作成されたキーファイルは、前記管理装置から前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは

記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

また、本発明の第 3 9 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

以下、本発明の第 3 9 の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格

納された前記コンテンツ鍵データおよび前記権利書データが復号し、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

また、本発明の第40の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

以下、本発明の第40の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱

いが決定される。

また、本発明の第41の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

以下、本発明の第41の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該作成されたキーファイルが前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

また、本発明の第42の観点のデータ提供システムは、データ提供装置からデ

ータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

以下、本発明の第42の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に配給される。

そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

データ提供システム。

また、本発明の第43の観点のデータ提供システムは、データ提供装置からデ

ータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

以下、本発明の第43の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

また、本発明の第44の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給

装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

以下、本発明の第44の観点のデータ提供システムの作用を説明する。

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールが、例えば、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して提供される。

次に、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納した第1のモジュールおよび第2のモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納することで、データ処理装置において、データ提供装置の関係者が作成した権利書データ

に基づいたコンテンツデータの取り扱い（利用）を行わせることが可能になる。

また、前記第 2 のモジュールは、所定の通信プロトコルに依存しない形式で前記データ配給装置から前記データ処理装置に配給されることから、前記第 2 のモジュールに格納されるコンテンツデータの圧縮方式や暗号化方式などを前記データ提供装置が任意に決定できる。

本発明の第 4 5 の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

以下、本発明の第 4 5 の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵データをを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールが提供される。

そして、前記データ配給装置から前記データ処理装置に、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いが決定される。

また、本発明の第46の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を

受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第 4 7 の観点のデータ提供システムは、データ提供装置から第 1 のデータ配給装置および第 2 のデータ配給装置にコンテンツデータを提供し、前記第 1 のデータ配給装置および前記第 2 のデータ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記第 1 のデータ配給装置、前記第 2 のデータ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記第 1 のデータ配給装置および前記第 2 のデータ配給装置に提供し、前記第 1 のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを前記データ処理装置に配給し、前記第 2 のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 3 のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第 2 のモジュールおよび前記第 3 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第 4 8 の観点のデータ提供システムは、第 1 のデータ提供装置からデータ配給装置に第 1 のコンテンツデータを提供し、第 2 のデータ提供装置からデータ配給装置に第 2 のコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記第 1 のデータ提供装置、前記第 2 のデータ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化さ

れた第1のコンテンツ鍵データと前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のキーファイルと、暗号化された第2のコンテンツ鍵データと前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のキーファイルとを作成し、前記第1のデータ提供装置は、前記第1のコンテンツ鍵データを用いて暗号化された前記第1のコンテンツデータを格納した第1のコンテンツファイルと、前記管理装置から受けた前記第1のキーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記第2のデータ提供装置は、前記第2のコンテンツ鍵データを用いて暗号化された前記第2のコンテンツデータを格納した第2のコンテンツファイルと、前記管理装置から受けた前記第2のキーファイルとを格納した第2のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のコンテンツファイル、前記第1のキーファイル、前記第2のコンテンツファイルおよび前記第2のキーファイルを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データ、前記第2のコンテンツ鍵データ、前記第1の権利書データおよび前記第2の権利書データを復号し、当該復号した第1の権利書データに基づいて前記第1のコンテンツデータの取り扱いを決定し、前記復号した第2の権利書データに基づいて前記第2のコンテンツデータの取り扱いを決定する。

また、本発明の第49の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテ

ンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第50の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第51の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであっ

て、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第52の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第53の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第54の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録し

て個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第55の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第56の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記

データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第56の観点のデータ提供システムは、好ましくは、前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する。

また、本発明の第56の観点のデータ提供システムは、好ましくは、前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する。

また、本発明の第57の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格

納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第58の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第59の観点のデータ提供システムは、データ提供装置、デー

タ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルを格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第60の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給

を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 6 1 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 6 2 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第63の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第64の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を

有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルを格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第65の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は

、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第66の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルに対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第67の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスソースに対応する前記管理装置に提供し、当該管理装置から受けたコン

テンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第68の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスタソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ

処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第69の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る。

また、本発明の第70の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであっ

て、前記データ提供装置は、コンテンツデータを提供し、前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する。

また、本発明の第34の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第35の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ

鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第36の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第37の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ

鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第38の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第39の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提

供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第40の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第41の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プ

ロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第42の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第43の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書デ

ータを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第44の観点のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第45の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを、前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュール

ルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第46の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第47の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ配給装置に配給し、前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第48の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイル

に格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第49の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第50の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテ

ンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第 5 1 の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第 5 2 の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データ

および前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第53の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第54の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用

いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第55の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテ

ンツデータの取り扱いを決定する。

また、本発明の第56の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第57の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当

該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第58の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第59の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツ

データの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第60の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第61の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用い

てコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第62の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ

処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第63の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第64の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイル

を作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第65の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給

を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第66の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第67の観点のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提

供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る。

また、本発明の第68の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータを提供し、前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する。

また、本発明の第71の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムであって、前記

データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第72の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第73の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記デ

ータ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した複数の第2のモジュールを、前記データ処理装置との間の相互認証によって得られた共有鍵を用いて暗号化した後に、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記複数の第2のモジュールを前記共有鍵を用いて復号し、当該復号した前記複数の第2のモジュールの中から単数または複数の第2のモジュールを選択し、前記第2のモジュールの配給サービスに対しての課金処理を行う第1の処理回路と、前記選択された前記第2のモジュールを受けて当該第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する耐タンパ性の第2の処理回路とを有する。

図面の簡単な説明

図1は、本発明の第1実施形態のEMDシステムの全体構成図であり、
図2は、本発明のセキュアコンテナの概念を説明するための図であり、
図3は、図1に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのSAMとの間で送受信されるデータに関連するデータの流れを示す図であり、

図4は、図1に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとEMDサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図であり、

図 5 は、図 1 に示すコンテンツプロバイダから S A M に送信されるセキュアコンテナのフォーマットを説明するための図であり、

図 6 は、図 5 に示すコンテンツファイルに含まれるデータを詳細に説明するための図であり、

図 7 は、図 5 に示すキーファイルに含まれるデータを詳細に説明するための図であり、

図 8 は、コンテンツファイルに格納されるヘッダデータを説明するための図であり、

図 9 は、コンテンツ I D を説明するための図であり、

図 1 0 は、セキュアコンテナのディレクトリ構造を説明するための図であり、

図 1 1 は、セキュアコンテナのハイパーリンク構造を説明するための図であり、

図 1 2 は、本実施形態で用いられる R O M 型の記録媒体の第 1 の例を説明するための図であり、

図 1 3 は、本実施形態で用いられる R O M 型の記録媒体の第 2 の例を説明するための図であり、

図 1 4 は、本実施形態で用いられる R O M 型の記録媒体の第 3 の例を説明するための図であり、

図 1 5 は、本実施形態で用いられる R A M 型の記録媒体の第 1 の例を説明するための図であり、

図 1 6 は、本実施形態で用いられる R A M 型の記録媒体の第 2 の例を説明するための図であり、

図 1 7 は、本実施形態で用いられる R A M 型の記録媒体の第 3 の例を説明するための図であり、

図 1 8 は、コンテンツプロバイダから E M D サービスセンタに送信される登録

要求用モジュールを説明するための図であり、

図19は、コンテンツプロバイダからEMDサービスセンタへの登録処理の手順を示すフローチャートであり、

図20は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートであり、

図21は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートであり、

図22は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートであり、

図23は、図1に示すEMDサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図であり、

図24は、図1に示すEMDサービスセンタの機能ブロック図であり、SAMおよび図1に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図であり、

図25は、図1に示すユーザホームネットワーク内のネットワーク機器の構成図であり、

図26は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテンツを復号するまでのデータの流れを示す図であり、

図27は、図25に示す外部メモリに記憶されるデータを説明するための図であり、

図28は、スタックメモリに記憶されるデータを説明するための図であり、

図29は、図1に示すユーザホームネットワーク内のネットワーク機器のその他の構成図であり、

図30は、図26に示す記憶部に記憶されるデータを説明するための図であり

図 3 1 は、図 1 に示すユーザホームネットワーク内の SAM の機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図であり、

図 3 2 は、図 2 5 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV 機器の SAM に転送する場合の転送元の SAM 内での処理の流れを説明するための図であり、

図 3 3 は、図 3 2 に示す場合における転送元の SAM 内でのデータの流れを示す図であり、

図 3 4 は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図であり、

図 3 5 は、図 3 2 に示す場合において、転送先の SAM において、入力したコンテンツファイルなどを、RAM 型あるいは ROM 型の記録媒体（メディア）に書き込む際のデータの流れを示す図であり、

図 3 6、コンテンツの購入形態が未決定の図 7 に示す ROM 型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV 機器において購入形態を決定する際の処理の流れを説明するための図であり、

図 3 7 は、図 3 6 に示す場合において、SAM 内でのデータの流れを示す図であり、

図 3 8 は、ユーザホームネットワーク内の AV 機器において購入形態が未決定の ROM 型の記録媒体からセキュアコンテナを読み出して、これを他の AV 機器に転送して RAM 型の記録媒体に書き込む際の処理の流れを説明するための図であり、

図 3 9 は、図 3 8 に示す場合における転送元の SAM 内でのデータの流れを示す図であり、

図 4 0 は、図 3 8 において、転送元の SAM から転送先の SAM に転送される

セキュアコンテナのフォーマットを説明するための図であり、

図 4 1 は、図 3 8 に示す場合における転送先の SAM 内でのデータの流れを示す図であり、

図 4 2 は、図 1 に示すコンテンツプロバイダ、EMD サービスセンタおよび SAM の相互間で、イン・バント方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図であり、

図 4 3 は、図 1 に示すコンテンツプロバイダ、EMD サービスセンタおよび SAM の相互間で、イン・バント方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図であり、

図 4 4 は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図であり、

図 4 5 は、SAM が作成する SAM 登録リストのデータフォーマットを説明するための図であり、

図 4 6 は、EMD サービスセンタが作成する SAM 登録リストのデータフォーマットを説明するための図であり、

図 4 7 は、図 1 に示すコンテンツプロバイダの全体動作のフローチャートであり、

図 4 8 は、第 1 実施形態の EMD システムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図であり、

図 4 9 は、本発明の第 1 実施形態の第 2 変形例を説明するための図であり、

図 5 0 は、本発明の第 1 実施形態の第 3 変形例を説明するための図であり、

図 5 1 は、本発明の第 1 実施形態の第 4 変形例において第 1 の手法を採用した場合を説明するための図であり、

図 5 2 は、本発明の第 1 実施形態の第 4 変形例において第 2 の手法を採用した場合を説明するための図であり、

図 5 3 は、本発明の第 1 実施形態の第 5 変形例を説明するための図であり、

図 5 4 は、本発明の第 1 実施形態の第 6 変形例の第 1 のパターンを説明するための図であり、

図 5 5 は、本発明の第 1 実施形態の第 6 変形例の第 2 のパターンを説明するための図であり、

図 5 6 は、本発明の第 1 実施形態の第 6 変形例の第 3 のパターンを説明するための図であり、

図 5 7 は、本発明の第 1 実施形態の第 6 変形例の第 4 のパターンを説明するための図であり、

図 5 8 は、本発明の第 1 実施形態の第 6 変形例の第 5 のパターンを説明するための図であり、

図 5 9 は、本発明の第 2 実施形態の EMD システムの全体構成図であり、

図 6 0 は、図 5 9 に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテンツに関するデータの流れを示す図であり、

図 6 1 は、コンテンツプロバイダにおいて行われるセキュアコンテンツの配送処理の手順を示すフローチャートであり、

図 6 2 は、コンテンツプロバイダにおいて行われるセキュアコンテンツの配送処理の手順を示すフローチャートであり、

図 6 3 は、図 5 9 に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図であり、

図 6 4 は、サービスプロバイダにおいて行われるセキュアコンテンツの作成処理の手順を示すフローチャートであり、

図 6 5 は、図 5 9 に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテンツのフォーマットを説明するための図であり、

図 6 6 は、図 6 5 に示すセキュアコンテンツに格納されたコンテンツファイルの送信形態を説明するための図であり、

図 6 7 は、図 6 5 に示すセキュアコンテナに格納されたキーファイルの送信形態を説明するための図であり、

図 6 8 は、図 5 9 に示すサービスプロバイダの機能ブロック図であり、EMD サービスセンタとの間で送受信されるデータの流れを示す図であり、

図 6 9 は、サービスプロバイダから EMD サービスセンタに送信されるブライスタグ登録要求用モジュールのフォーマットを説明するための図であり、

図 7 0 は、図 5 9 に示す EMD サービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図であり、

図 7 1 は、図 5 9 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図であり、

図 7 2 は、図 5 9 に示す EMD サービスセンタの機能ブロック図であり、SAM との間で送受信されるデータに関連するデータの流れを示す図であり、

図 7 3 は、利用履歴データの内容を説明するための図であり、

図 7 4 は、図 5 9 に示すネットワーク機器の構成図であり、

図 7 5 は、図 7 4 に示す CA モジュールの機能ブロック図であり、

図 7 6 は、図 7 4 に示す SAM の機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図であり、

図 7 7 は、図 7 6 に示す記憶部に記憶されるデータを説明するための図であり

図 7 8 は、図 7 4 に示す SAM の機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図であり、

図 7 9 は、SAM におけるセキュアコンテナの購入形態の決定処理の手順を示すフローチャートであり、

図 8 0 は、購入形態が決定された後のキーファイルのフォーマットを説明する

ための図であり、

図 8 1 は、図 7 4 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に入力形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送先のSAM内での処理の流れを説明するための図であり、

図 8 2 は、図 8 1 に示す場合の転送元のSAM内でのデータの流れを示す図であり、

図 8 3 は、図 8 1 に示す場合の転送先のSAM内でのデータの流れを示す図であり、

図 8 4 は、図 5 9 に示すEMDシステムの全体動作のフローチャートであり、

図 8 5 は、図 5 9 に示すEMDシステムの全体動作のフローチャートであり、

図 8 6 は、第 2 実施形態のEMDシステムにおけるサービスプロバイダからユーザホームネットワークへのセキュアコンテンツの配送形態の一例を説明するための図であり、

図 8 7 は、第 2 実施形態のEMDシステムが採用するセキュアコンテンツの配送プロトコルの一例を説明するための図であり、

図 8 8 は、図 8 7 においてユーザホームネットワークからサービスプロバイダ 3 1 0 へのセキュアコンテンツなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 8 9 は、図 8 7 においてコンテンツプロバイダからEMDサービスセンタへのキーファイルなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 0 は、図 8 7 においてサービスプロバイダからEMDサービスセンタへのプライスタグデータ 3 1 2 などを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 1 は、図 8 7 においてユーザホームネットワーク内でセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 2 は、デジタル放送のデータ放送方式に XML / SMIL / BML を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図であり、

図 9 3 は、デジタル放送のデータ放送方式に MHEG を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図であり、

図 9 4 は、インターフェイスのデータ放送方式に XML / SMIL を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図であり、

図 9 5 は、ユーザホームネットワークから EMD サービスセンタに利用履歴データなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 6 は、ユーザホームネットワーク内においてセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図であり、

図 9 7 は、本発明の第 2 実施形態の第 1 変形例に係わる 2 個のサービスプロバイダを用いた EMD システムの構成図であり、

図 9 8 は、本発明の第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いた EMD システムの構成図であり、

図 9 9 は、本発明の第 2 実施形態の第 3 変形例に係わる EMD システムの構成図であり、

図 1 0 0 は、本発明の第 2 実施形態の第 4 変形例に係わる EMD システムの構成図であり、

図 1 0 1 は、公開鍵証明書データの取得ルートの形態を説明するための図であり、

図102は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図であり、

図103は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図であり、

図104は、SAMの公開鍵証明書データを無効にする場合の処理を説明するための図であり、

図105は、SAMの公開鍵証明書データを無効にする場合のその他の処理を説明するための図であり、

図106は、図47に示すEMDシステムにおいて、EMDサービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図であり、

図107は、図106に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体のEMDサービスセンタ内に設けた場合のEMDシステムの構成図であり、

図108は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のEMDシステムの構成図であり、

図109は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のEMDシステムの構成図であり、

図110は、コンテンツプロバイダが権利管理用クリアリングハウスおよび電子決済用クリアリングハウスの双方の機能をさらに備えている場合のEMDシステムの構成図であり、

図111は、本発明の第2実施形態の第8変形例において、図47に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテンツのフォーマットを説明するための図であり、

図112は、図111に示すコンテンツファイルとキーファイルとの間のディレクトリ構造データによるリンク関係を説明するための図であり、

図 1 1 3 は、コンテンツファイルとキーファイルとの間のディレクトリ構造のその他の例を説明するための図であり、

図 1 1 4 は、本発明の第 2 実施形態の第 8 変形例において、図 4 7 に示すサードプロバイダから SAM に提供されるセキュアコンテナのフォーマットを説明するための図であり、

図 1 1 5 は、コンボジット型のセキュアコンテナのデータフォーマットの第 1 の概念を説明するための図であり、

図 1 1 6 は、コンボジット型のセキュアコンテナのデータフォーマットの第 2 の概念を説明するための図であり、

図 1 1 7 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいて第 1 の手法を採用した場合を説明するための図であり、

図 1 1 8 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいて第 2 の手法を採用した場合を説明するための図であり、

図 1 1 9 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいてファイル形式を採用しない場合のデータフォーマットを説明するための図であり、

図 1 2 0 は、本発明の第 2 実施形態の第 1 0 変形例に係わる EMD システムの構成図であり、

図 1 2 1 は、本発明の第 2 実施形態の第 1 1 変形例の第 1 のパターンに係わる EMD システムの構成図であり、

図 1 2 2 は、本発明の第 2 実施形態の第 1 1 変形例の第 2 のパターンに係わる EMD システムの構成図であり、

図 1 2 3 は、本発明の第 2 実施形態の第 1 1 変形例の第 3 のパターンに係わる EMD システムの構成図であり、

図 1 2 4 は、本発明の第 2 実施形態の第 1 1 変形例の第 4 のパターンに係わる EMD システムの構成図であり、

図125は、本発明の第2実施形態の第11変形例の第5のパターンに係わるEMDシステムの構成図であり、

図126は、本発明の第2実施形態の第9変形例に係わるEMDシステムの構成図であり、

図127は、本発明の第2実施形態におけるセキュアコンテナのファイル包括大小関係を説明するための図であり、

図128は、本発明の第3実施形態のEMDシステムを説明するための図であり、

図129は、図128に示すEMDサービスセンタの機能ブロック図であり、

図130は、本発明の第3実施形態のEMDシステムの変形例を説明するための図であり、

図131は本発明の第4実施形態のEMDシステムを説明するための図であり、

図132は本発明の第4実施形態のEMDシステムの変形例を説明するための図であり、

図133は本発明の第5実施形態のEMDシステムを説明するための図であり、

図134は本発明の第5実施形態のEMDシステムの変形例を説明するための図であり、

図135は本発明の第5実施形態のEMDシステムのその他の変形例を説明するための図であり、

図136は本発明の第6実施形態のEMDシステムを説明するための図であり、

図137は本発明の第6実施形態のEMDシステムの変形例を説明するための図であり、

図 1 3 8 は本発明の第 6 実施形態の EMD システムのその他の変形例を説明するための図であり、

図 1 3 9 は本発明の第 7 実施形態の EMD システムを説明するための図であり、

図 1 4 0 は本発明の第 7 実施形態の EMD システムの変形例を説明するための図であり、

図 1 4 1 は本発明の第 7 実施形態の EMD システムのその他の変形例を説明するための図であり、

図 1 4 2 は本発明の第 8 実施形態の EMD システムを説明するための図であり、

図 1 4 3 は本発明の第 9 実施形態の EMD システムを説明するための図であり、

図 1 4 4 は、コンテンツプロバイダにおいてキーファイルを作成した場合のキーファイルのフォーマットを説明するための図であり、

図 1 4 5 は、従来の EMD システムの構成図である。

発明を実施するための最良の形態

以下、本発明の実施形態に係わる EMD (Electronic Music Distribution: 電子音楽配信) システムについて説明する。

第 1 実施形態

図 1 は、本実施形態の EMD システム 1 0 0 の構成図である。

本実施形態において、ユーザに配信されるコンテンツ (Content) データとは、情報そのものが価値を有するデジタルデータをいい、画像データ、オーディオデータ、プログラム (ソフトウェア) などがあるが、以下、音楽データを例に説明する。

図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ（クリアリング・ハウス、以下、ESCとも記す）102およびユーザホームネットワーク103を有する。

ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM105₁～105₄が、それぞれ請求項1、請求項6、請求項104および請求項109などに係わるデータ提供装置、管理装置およびデータ処理装置に対応している。

先ず、EMDシステム100の概要について説明する。

EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCを暗号化する際に用いたコンテンツ鍵データK_c、コンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある権威機関であるEMDサービスセンタ102に送る。

EMDサービスセンタ102は、コンテンツプロバイダ101から受けたコンテンツ鍵データK_c、権利書データ106並びに電子透かし情報鍵データを登録（認証および権威化）する。

また、EMDサービスセンタ102は、対応する期間の配信用鍵データKD₁～KD₅で暗号化したコンテンツ鍵データK_c、権利書データ106および自らの署名データなどを格納したキーファイルKFを作成し、これをコンテンツプロバイダ101に送る。

ここで、当該署名データは、キーファイルKFの改竄の有無、キーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102において正規に登録されたことを検証するために用いられる。

また、コンテンツプロバイダ101は、コンテンツ鍵データK_cでコンテンツデータCを暗号化してコンテンツファイルCFを生成し、当該生成したコンテン

ツファイルCFと、EMDサービスセンタ102から受けたキーファイルKFと、自らの署名データなどを格納したセキュアコンテナ（本発明のモジュール）104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク103に配給する。

ここで、セキュアコンテナ104内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

ユーザホームネットワーク103は、例えば、ネットワーク機器160₁およびAV機器160₂～160₄を有する。

ネットワーク機器160₁は、SAM(Secure Application Module)105₁を内蔵している。

AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。SAM105₁～105₄相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルインタフェースバスなどのバス191を介して接続されている。

SAM105₁～105₄は、ネットワーク機器160₁がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および／または、コンテンツプロバイダ101からAV機器160₂～160₄に記録媒体を介してオフラインで供給されたセキュアコンテナ104に対応する期間の配信用鍵データKD₁～KD₃を用いて復号した後に、署名データの検証を行う。

SAM105₁～105₄に供給されたセキュアコンテナ104は、ネットワーク機器160₁およびAV機器160₂～160₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。



(57) 要約:

データ提供装置の関係者の利益を保護できるデータ提供システムを提供する。コンテンツプロバイダ101は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、配信鍵用データを用いて暗号化されたコンテンツ鍵データと、コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したセキュアコンテナ104をユーザホームネットワーク103のSAM105₁などに配給する。SAM105₁などは、セキュアコンテナ104に格納されたコンテンツ鍵データおよび権利書データを復号し、当該復号した権利書データに基づいて、コンテンツデータの購入形態および利用形態などの取り扱いを決定する。

明細書

データ提供システムおよびその方法

技術分野

本発明は、コンテンツデータを提供するデータ提供システムおよびその方法と、データ提供装置と、データ処理装置とに関する。

背景技術

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来のEMD (Electronic Music Distribution: 電子音楽配信) システムがある。

図145は、従来のEMDシステム700の構成図である。

図145に示すEMDシステム700では、コンテンツプロバイダ701a, 701bが、サービスプロバイダ710に対し、コンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報705a, 705b, 705cには、例えば、SCMS (Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ710の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

サービスプロバイダ710は、受信したコンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとをセッション鍵データを用いて復号する。

そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a, 704b, 704cに、著作権情報705a, 705b, 705cを埋め込んで、コンテンツデータ707a, 707b, 707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a, 705b, 705cのうち電子透かし情報をコンテンツデータ704a, 704b, 704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。

さらに、サービスプロバイダ710は、コンテンツデータ707a, 707b, 707cを、鍵データベース706から読み出したコンテンツ鍵データKca, Kcb, Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a, 707b, 707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA(Conditional Access)モジュール711に送信する。

CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca, Kcb, Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a, 707b, 707cを、それぞれコンテンツ鍵データKca, Kcb, Kccを用いて復号することが可能になる。

このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ710の権利処理モジュール720に送信する。

この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービスプロバイダ710とコンテンツプロバイダ701a, 701b, 701cとの間で利益分配を行う。

このとき、サービスプロバイダ710から、コンテンツプロバイダ701a, 701b, 701cへの利益分配は、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)を介して行われる。また、JASRACによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

また、端末装置709では、コンテンツ鍵データKca, Kcb, Kccを用いて復号したコンテンツデータ707a, 707b, 707cを、RAM型の記録媒体723などに記録する際に、著作権情報705a, 705b, 705cのSCMSビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ707a, 707b, 707cに埋め込まれたSCMSビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

ところで、SCMSは、コンテンツデータを例えば2世代以上のわたって複製することを禁止するものであり、1世代の複製は無限に行うことができ、著作権者の保護として不十分であるという問題がある。

また、上述したEMDシステム700では、サービスプロバイダ710が暗号

化されていないコンテンツデータを技術的には自由に扱えるため、コンテンツプロバイダ701の関係者はサービスプロバイダ710の行為等を監視する必要があり、当該監視の負担が大きいと共に、コンテンツプロバイダ701の利益が不当に損なわれる可能性が高いという問題がある。

また、上述したEMDシステム700では、ユーザの端末装置709がサービスプロバイダ710から配給を受けたコンテンツデータをオーサリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ701の利益が不当に損なわれるという問題がある。

発明の開示

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システムおよびその方法を提供することを目的とする。

また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システムおよびその方法を提供することを目的とする。

上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第1の観点のデータ提供システムは、好ましくは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づい

て、前記コンテンツデータの取り扱いを決定する。

本発明の第1の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータが提供される。

そして、前記データ処理装置において、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

また、本発明の第2の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

本発明の第2の観点のデータ提供システムの作用は以下に示すようになる。

管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。

そして、当該作成されたキーファイルが、前記管理装置から前記データ提供装

置に配給される。

そして、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールが、前記データ提供装置から前記データ処理装置に配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

本発明の第3の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

本発明の第3の観点のデータ提供システムの作用は以下に示ようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキー

ファイルとを含むコンテンツファイルを格納したモジュールが配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号され権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

また、本発明の第4の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

本発明の第4の観点のデータ提供システムの作用は以下に示ようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとが配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納

されたコンテンツデータの取り扱いが決定される。

また、本発明の第5の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

本発明の第5の観点のデータ提供システムの作用は以下に示ようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。

当該作成されたキーファイルは、前記管理装置から前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルが配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

また、本発明の第6の観点のデータ提供システムは、データ提供装置からデー

タ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

本発明の第6の観点のデータ提供システムの作用は以下に示ようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールが配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号し、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

。

また、本発明の第7の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、

前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

本発明の第7の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとが個別に配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いが決定される。

また、本発明の第8の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

本発明の第 8 の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該作成されたキーファイルが前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

また、本発明の第 9 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

本発明の第 9 の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵デ

ータを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとが個別に配給される。

そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

また、本発明の第10の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

本発明の第10の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが配給される。

そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、

前記配給を受けた前記コンテンツデータの取り扱いが決定される。

また、本発明の第11の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

本発明の第11観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。

そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータが提供される。

そして、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータが配給される。

そして、前記データ処理装置において、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いが決定される。

また、本発明の第12の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理

装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

本発明の第12の観点のデータ提供システムの作用は以下に示ようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールが提供される。

そして、前記データ配給装置から前記データ処理装置に、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールが配給される。

そして、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当

該復号された権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いが決定される。

また、本発明の第13の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第14の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ処理

装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第15の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第16の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受

けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第17の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第18の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを前記デ

ータ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第19の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第20の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受

けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第21の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第22の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、

前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第23の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第24の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は

、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 25 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 26 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ

提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第27の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第28の観点のデータ提供システムは、複数のデータ提供装置

、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第29の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前

記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第30の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第31の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り

扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルに対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第32の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスターソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルに対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第33の観点のデータ提供システムは、複数のデータ提供装置

、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第1の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第2の観点のデータ提供方法は、データ提供装置からデータ処

理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第3の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第4の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す

暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第5の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第6の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータ

と、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、本発明の第7の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第8の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り

扱いを決定する。

また、本発明の第 9 の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 10 の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

また、本発明の第 11 の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供システムであって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成

し、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを前記データ提供装置から前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第12の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを、前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第13の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記

管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第14の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ配給装置に配給し、前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第15の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルを前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第16の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受け

た前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

また、本発明の第17の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第18の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コ

ンテンツデータの取り扱いを決定する。

また、本発明の第 19 の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

また、本発明の第 20 の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コン

テンツデータの取り扱いを決定する。

また、本発明の第 2 1 の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 2 2 の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を

受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第23の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第24の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置

から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第25の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第26の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納

し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 27 の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 28 の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコ

ンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第2の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 30 の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第 31 の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルに対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテ

ンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第32の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスタソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルの前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルに対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第33の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスタソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツフ

ファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

また、本発明の第34の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供であって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

本発明の第34の観点のデータ提供システムの作用は以下に示すようになる。

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前

記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールが配給される。

このとき、当該モジュールは、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式、あるいは記録媒体に記録されて前記データ提供装置から前記データ処理装置に配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納したモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納することで、データ処理装置において、データ提供装置の関係者が作成した権利書データに基づいたコンテンツデータの取り扱い（利用）を行わせることが可能になる。

また、前記モジュールは、所定の通信プロトコルに依存しない形式で前記データ提供装置から前記データ処理装置に配給されることから、前記モジュールに格納されるコンテンツデータの圧縮方式や暗号化方式などを前記データ提供装置が任意に決定できる。

また、本発明の第34の観点のデータ提供システムは、好ましくは、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記モジュールを前記データ処理装置に配給する。

また、本発明の第34の観点のデータ提供システムは、好ましくは、前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて、当該データが改竄されていないかを検証するためのデータと、当該データを所定の機関によって正規に認証されているかを検証するための署名データとのうち少なくとも一方のデータをさらに格納した前記モジュールを前記データ処理装置に配給する。

また、本発明の第 3 4 の観点のデータ提供システムは、好ましくは、前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態を決定し、前記コンテンツデータを他のデータ処理装置に転送する場合に、当該コンテンツデータの購入者の正当性を示す署名データと、当該コンテンツデータの送信者の正当性を示す署名データとを異ならせる。

本発明の第 3 5 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

本発明の第 3 5 の観点のデータ提供システムの作用は以下に示すようになる。

管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。

そして、当該作成されたキーファイルが、前記管理装置から前記データ提供装置に配給される。

そして、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格

納したモジュールが、前記データ提供装置から前記データ処理装置に所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

また、本発明の第35の観点のデータ提供システムは、好ましくは、前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する。

また、本発明の第35の観点のデータ提供システムは、好ましくは、前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する。

また、本発明のデータ提供装置は、管理装置によって管理され、データ処理装置にコンテンツデータを配給するデータ提供装置であって、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを前記管理装置から受け、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給する。

また、本発明のデータ処理装置は、管理装置によって管理され、コンテンツデータを利用するデータ処理装置であって、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルと、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータ